Avira Premium Security Suite
使用手冊



商標與著作權

商標

著作權資訊

目錄

1 簡介

您的 AntiVir 程式可保護您的電腦免於各種病毒、蠕蟲、木馬程式、廣告軟體和間諜軟體與其他各種危險的入侵。在本手冊中，這些統稱病毒或惡意程式碼 (有害軟體) 和有害程式。

本手冊說明程式安裝與操作方式。

如需了解更多選項和資訊，請造訪我們的網站：

http://www.avira.tw

您可以在 Avira 網站進行下列作業......

– 存取其他 AntiVir 桌面程式的相關資訊
– 下載最新版的 AntiVir 桌面程式
– 下載 PDF 格式的最新產品手冊
– 下載免費的支援和修復工具
– 存取我們的全方位知識庫和常見問題集 (FAQ) 進行疑難排解
– 存取特定國家支援服務地址。

Avira 團隊敬上

2 圖示與強調樣式

下列為使用的圖示：

圖示/指定	說明
✓	如果必須先滿足某項條件才能執行某項動作，就會放置此圖示。
▶	放置在您執行某項動作步驟的前面。
→	在上一個動作之後發生的事件之前，會放置此圖示。
警告	在針對重要資料遺失危險提出警告之前，會放置此圖示。
注意	放置在有利於使用 AntiVir 程式的特別重要資訊或提示之連結前面。

下列為使用的強調樣式：

強調樣式	說明
書寫體	檔名或路徑資料。
	顯示的軟體介面元素 (例如，視窗標題、視窗欄位或選項方塊)。
粗體	可按一下的軟體介面元素 (例如，功能表項目、區段或按鈕)。

3 產品資訊

本章包含購買與使用 AntiVir 產品的所有相關資訊：

– 請參閱下列章節：提供的功能
– 請參閱下列章節：系統需求
– 請參閱下列章節：授權
– 請參閱下列章節： 授權管理員

AntiVir 程式內含完整、彈性的工具，可供您放心地用來保護電腦免於各種病毒、惡意程式碼、有害程式與其他危險的入侵。

▶ 請注意下列資訊：

注意
遺失寶貴的資料通常會帶來無法想像的後果。即使是最好的防毒程式也無法 100% 保證免於資料遺失的風險。定期複製 (備份) 資料以策安全。

注意
要可靠且有效地防範病毒、惡意程式碼、有害程式與其他危險，必須使用最新的程式方能奏效。請務必使用自動更新將 AntiVir 程式維持在最新狀態。請依據需求設定程式。

3.1 提供的功能

您的 AntiVir 程式包含下列功能：

– 用於監視、管理與控制整個程式的控制中心
– 透過使用者友善標準與進階選項和即時線上說明來集中設定
– 掃描程式 (指定掃描) 搭配由設定檔控制且可設定的掃描，可掃描所有已知的病毒和惡意程式碼類型
– 與 Windows Vista 使用者帳戶控制的整合可讓您執行需要系統管理員權限的工作。
– Guard (即時掃描) 可持續監視所有檔案存取活動
– ProActiv 元件可永久監視程式動作 (只適用於 32 位元系統，不適用於 Windows 2000)
– MailGuard (POP3 掃描程式、IMAP 掃描程式 和 SMTP 掃描程式) 可隨時檢查電子郵件中的病毒與惡意程式碼。包含檢查電子郵件附件的功能
– WebGuard 可監視透過 HTTP 通訊協定從網際網路傳輸的資料與檔案 (監視連接埠 80、8080、3128)
– 家長監護元件可依據不同的角色，篩選不適當的網站及限制網際網路的使用。
– 備份元件可為您的資料建立備份 (鏡像備份)
– 可隔離與處理可疑檔案的整合式隔離區管理

- Rootkit 保護機制可偵測安裝在電腦系統中的隱藏惡意程式碼 (Rootkit) (不適用於 Windows XP 64 位元)
- 可透過網際網路，針對偵測到的病毒與惡意程式碼直接存取其詳細資訊
- 經由網際網路上的網路伺服器，以單一檔案更新或增量 VDF 更新方式，簡單、快速地更新程式、病毒定義與搜尋引擎
- 授權管理員中使用者友善的授權方式
- 整合式排程管理員可規劃單次或重複性工作，例如更新或掃描
- 透過創新的掃描技術 (掃描引擎，包括啓發式掃毒)，達到極高的病毒與惡意程式碼偵測水準
- 可偵測所有典型的封存類型，包括偵測巢狀式封存與智慧副檔名偵測
- 高效能的多執行緒功能 (同時高速掃描多個檔案)
- Avira FireWall 可保護您的電腦免於透過網際網路或另一個網路的未授權存取，並防範未授權使用者對網際網路或內部網路進行未授權存取。

3.2 系統需求

下面列出系統需求：

- Pentium 等級或更新的電腦，至少 266 MHz
- 作業系統
- Windows XP SP2 (32 或 64 位元) 或
- Windows Vista (32 或 64 位元，加裝 SP 1)
- Windows 7 (32 或 64 位元)
- 至少 150 MB 的可用硬碟記憶體空間 (如果使用 [隔離區] 做爲暫存區域的話，就需要更多記憶體)
- Windows XP 環境下，至少需要 256 MB 的記憶體
- - Windows Vista、Windows 7、Windows Server 2008 與 Windows Server 2008 R2 環境下，至少需要 1024 MB 記憶體
- 程式安裝：系統管理員權限
- 所有安裝：Windows Internet Explorer 6.0 或更新的版本
- 必要時，提供網際網路連線 (請參閱安裝)

3.3 授權與升級

若要使用 AntiVir 產品，您需要一份授權。請藉此接受授權條款。

授權會以啓用金鑰形式來提供。啓用金鑰是當您購買 AntiVir 產品之後將收到的一個由字母和數字組成的代碼。啓用金鑰內含您的授權詳細資料，亦即獲得了哪些程式授權與其授權期間。

如果您透過網路商店購買 AntiVir 產品，將會經由電子郵件收到啓用金鑰，否則會直接附在產品包裝上。

若要授權程式，請輸入啓用金鑰以啓用程式。您可以在安裝期間執行產品啓用程序。不過，您也可以在安裝之後，透過授權管理員的 [說明]::[授權管理] 來啓用 AntiVir 程式。

您可以在授權管理員選擇從 AntiVir 桌面產品系列啓動產品升級。不需要手動解除安裝舊產品及手動安裝新產品。從授權管理員升級時，只要在 [授權管理員] 輸入方塊中輸入要升級之產品的啓用代碼。新產品隨即自動安裝。

下列產品升級可透過授權管理員自動執行：

– Avira AntiVir Personal 升級爲 Avira AntiVir Premium
– Avira AntiVir Personal 升級爲 Avira Premium Security Suite
– Avira AntiVir Premium 升級爲 Avira Premium Security Suite

4 安裝與解除安裝

本章包含安裝與解除安裝 AntiVir 程式的相關資訊。

- 請參閱下列章節：安裝：條件、安裝類型、安裝
- 請參閱下列章節：安裝模組
- 請參閱下列章節：修改安裝
- 請參閱下列章節：解除安裝：解除安裝

4.1 安裝

在安裝之前，請檢查您的電腦是否滿足所有的基本系統需求。如果您的電腦滿足所有需求，就可以安裝 AntiVir 程式。

> **注意**
> 在安裝過程期間，您可以選擇建立還原點。還原點的設置目的是要用來將作業系統重設回其預先安裝狀態。如果您要使用這個選項，請確定作業系統允許建立還原點：
> Windows XP：系統內容 -> 系統還原：停用此選項：**停用系統還原**。
> Windows Vista/Windows 7：系統內容 -> 電腦保護：在 **[保護設定]** 區域中，反白系統安裝所在的磁碟機，並且按一下 **[設定]** 按鈕。啟用 **[系統保護]** 視窗中的選項 **[系統設定和還原至先前檔案版本]**。

安裝類型

您可以在安裝期間，在安裝精靈中選取一種安裝類型：

<u>快速安裝</u>

- 並未安裝所有程式元件。下列程式元件未安裝：

  Avira AntiVir ProActiv

  Avira FireWall

- 程式檔案會安裝至 `C:\Program Files` 底下的指定預設資料夾中。
- 您的 AntiVir 程式會以預設設定進行安裝。您可以選擇使用組態精靈定義自訂設定。

<u>使用者定義</u>

- 您可以選擇安裝個別的程式元件 (請參閱安裝與解除安裝::安裝模組)。
- 您可以針對要安裝的程式檔案，選取目標資料夾。
- 您可以選擇不要建立桌面圖示和 [開始] 功能表中的程式群組。
- 您可以使用組態精靈，定義 AntiVir 程式的自訂設定，並啟始安裝後自動執行的快速系統掃描。

開始安裝之前

- 關閉您的電子郵件程式。同時建議您結束所有執行中的應用程式。
- 確定沒有安裝其他防毒解決方案。不同的資訊安全解決方案的自動保護功能可能會互相影響。
- 建立網際網路連線：您需要網際網路連線以執行下列安裝步驟：
- 針對網際網路型態的安裝並經由安裝程式下載最新的程式檔案與掃描引擎，以及最新的病毒定義檔
- 啓動程式
- 完成安裝後，請適當地執行更新。
- 當您要啓動程式時，請備妥 AntiVir 程式的授權金鑰。

注意
網際網路型態的安裝：
針對程式的網際網路型態安裝提供一項安裝程式，此安裝方式會在 Avira GmbH 網路伺服器執行安裝作業之前載入最新的程式檔案。 此程序可確保安裝的 AntiVir 程式內含最新的病毒定義檔。
使用安裝套件來安裝：
安裝套件同時包含安裝程式與所有必要的程式檔案。安裝套件不包含任何可用的 AntiVir 程式安裝語言選項。建議您在安裝之後，執行病毒定義檔更新。

注意
啓用產品時，AntiVir 程式會使用 HTTP 通訊協定與連接埠 80 (網路通訊)，並搭配加密通訊協定 SSL 與連接埠 443，以便和 Avira GmbH 伺服器通訊。 如果您是使用防火牆，請確保必要的連線與/或傳入或傳出的資料沒有遭到防火牆封鎖。

安裝

安裝程式會執行自我說明的對話模式。每個視窗都包含可控制安裝處理序的特定按鈕選項。

下列功能會指派給最重要的按鈕：

- **確定**：確認動作。
- **中止**：中止動作。
- **下一步**：移至下一個步驟。
- **上一步**：移至上一個步驟。

安裝您的 AntiVir 程式：

注意
下列 Windows FireWall 停用動作僅適用 Windows XP 作業系統。

- 按兩下剛從網際網路下載的安裝檔案，或是插入程式光碟，以啓動安裝程式。

網際網路型態的安裝

[歡迎使用] 對話方塊隨即顯示。

- 按 **[下一步]** 繼續安裝。

[語言選擇] 對話方塊隨即顯示。

- 選取您要用來安裝 AntiVir 程式的語言，並按 **[下一步]** 確認語言選擇。

[下載] 對話方塊隨即顯示。Avira GmbH 網路伺服器會開始下載所有必要的

安裝檔案。*[下載]* 視窗會在下載結束時關閉。

<u>使用安裝套件來安裝</u>

安裝精靈開啓時會顯示 *Avira Premium Security Suite* 對話方塊。

▶ 按一下 *[接受]* 開始安裝。

這時會開始解壓縮安裝檔案。安裝常式正式開始。

[歡迎使用] 對話方塊隨即顯示。

▶ 按 **[下一步]**。

<u>繼續進行網際網路型態的安裝，以及使用安裝套件進行的安裝作業</u>

這時會顯示內含授權合約的對話方塊。

▶ 確認接受授權合約，並按一下 **[下一步]**。

[產生序號] 對話方塊隨即顯示。

▶ 必要時，請確認已在更新期間產生亂數序號並傳輸成功，然後按一下 **[下一步]** 。

[選取安裝類型] 對話方塊隨即顯示。

▶ 啓用選項 **[快速安裝]** 或 **[使用者定義]**。如果您要建立還原點，請啓用選項 **[建立系統還原點]**。按 **[下一步]** 確認您的設定。

<u>使用者定義的安裝</u>

[選取目的地目錄] 對話方塊隨即顯示。

▶ 按 **[下一步]**，確認指定的目的地目錄。

- 或 -

使用 **[瀏覽]** 按鈕選取其他目的地目錄，並按 **[下一步]** 確認動作。

[安裝元件] 對話方塊隨即顯示：

▶ 啓用或停用所需的元件，並按一下 **[下一步]** 確認動作。

如果您選擇了安裝 ProActiv 元件，*[AntiVir ProActiv 社群]* 視窗隨即開啓。您可以選擇確認參加 Avira AntiVir ProActiv 社群：如果此選項已經啓用，Avira AntiVir ProActiv 會將 ProActiv 元件偵測到的可疑程式資訊傳送至 Avira 惡意程式碼研究中心。這份資料只會用於進階線上掃描，以及擴展和調整偵測技術。您可以使用**詳細資訊**連結，取得關於已擴充線上掃描的詳細資訊。

▶ 啓用或停用參加 AntiVir ProActiv 社群，並按 **[下一步]** 確認。

您可以在下列對話方塊中，決定是否建立桌面捷徑與/或在 [開始] 功能表中建立程式群組。

▶ 按 **[下一步]**。

▶ 略過下一節＜快速安裝＞。

<u>快速安裝</u>

[AntiVir ProActiv 社群] 視窗隨即開啓。您可以選擇確認參加 Avira AntiVir ProActiv 社群：如果此選項已經啓用，Avira AntiVir ProActiv 會將 ProActiv 元件偵測到的可疑程式資訊傳送至 Avira 惡意程式碼研究中心。這份資料只會用於進階線上掃描，以及擴展和調整偵測技術。您可以使用**詳細資訊**連結，取得關於已擴充線上掃描的詳細資訊。

▶ 啓用或停用參加 AntiVir ProActiv 社群，並按 **[下一步]** 確認。

<u>繼續：快速安裝與使用者定義的安裝</u>

授權精靈隨即開啓。

您可以透過下列選項來啓用程式。

- 輸入啓用金鑰。

  輸入啓用金鑰後，AntiVir 程式可使用您的授權來啓用。

- 選取 **[產品測試]** 選項

  一旦您選取 **[產品測試]**，啓用程序期間便會產生一份評估授權，供您用來啓用程式 。您可以在特定期限內測試 AntiVir 程式的完整功能。

注意
您可以透過 **[有可用的有效 hbedv.key 授權檔] 選項，載入有效的授權檔。**使用有效的啓用金鑰來啓用產品時，系統會產生授權金鑰並儲存在您的 AntiVir 程式目錄中。如果您已經啓用產品，而想要重新安裝 AntiVir 程式，請使用這個選項。

注意
在某些 AntiVir 產品銷售版本中，產品會內附啓用金鑰。此時您無須輸入啓用金鑰。有需要的話，啓用金鑰會顯示在授權精靈中。

注意
若要啓用程式，您需要與 Avira GmbH 伺服器建立連線。在 **[Proxy 設定]** 底下，您可以設定 Proxy 伺服器的網際網路連結。

▶ 選取啓用程序並按 **[下一步]** 確認動作。

產品啓用

這時會開啓一個對話方塊，供您輸入個人資料。

▶ 輸入個人資料，並按**[下一步]**

您的資料已經傳輸到 Avira GmbH 伺服器並進行掃描。您的 AntiVir 已經透過授權完成啓用。

您的授權資料會顯示在下一個視窗中。

▶ 按 **[下一步]**。

▶ 略過以下章節：選取 **[有可用的有效 hbedv.key]** 選項以啓用產品。""

選取 [有可用的有效 **hbedv.key**] 選項

隨即開啓一個方塊，供您載入授權檔案。

▶ 選取程式專用且內含授權資料的授權檔 hbedv.key，然後按一下 **[開啓]**

您的授權資料會顯示在下一個視窗中。

▶ 按 **[下一步]**

在完成啓用或載入授權檔之後繼續進行

將會安裝所有的程式功能。安裝進度會顯示在對話方塊中。

您可以在下列對話方塊中，選擇是否要在安裝完成後開啓讀我檔案，以及是否要重新啓動電腦。

▶ 必要時同意選項並按一下 *[完成]* 完成安裝。

這時會關閉安裝精靈。

繼續：使用者定義的安裝
組態精靈

如果您選擇使用者定義的安裝，下列步驟會開啓組態精靈。組態精靈可讓您定義您的 AntiVir 程式的自訂設定。

▶ 在組態精靈的歡迎使用視窗中，按 **[下一步]**，開始進行程式的組態設定。

[設定 AHeAD] 對話方塊可讓您針對 AHeAD 技術選取一項偵測等級。選取的偵測等級將用於掃描程式 (指定掃描) 與 Guard (即時掃描) AHeAD 技術設定。

▶ 選取一項偵測等級，並按 **[下一步]** 繼續安裝。

在接下來的 *[選取延伸的威脅類別]* 對話方塊中，您可以依據指定的威脅類別調整 AntiVir 程式保護功能。

▶ 必要時啓用進一步威脅類別並按 *[下一步]* 繼續安裝。

如果您已選取 AntiVir FireWall 安裝模組，*[FireWall 安全性等級]* 對話方塊會出現。您可以定義 Avira FireWall 是否應該允許外部存取啓用的資源，並允許信任的公司應用程式進行網路存取活動。

▶ 啓用所需選項，並按 *[下一步]*，繼續進行組態設定。

如果您已選取 AntiVir Guard 安裝模組，*[Guard 啓動模式]* 對話方塊會出現。您可以規範 Guard 啓動時間。每次電腦重新開機時，Guard 會以指定的啓動模式來啓動。

注意
指定的 Guard 啓動模式會儲存在登錄中，而且無法經由 [組態] 變更。

▶ 啓用所需選項，並按 *[下一步]*，繼續進行組態設定。

如果您已選取 AntiVir WebGuard 安裝模組，*[啓用家長監護]* 對話方塊會出現。您可以規範 Guard 啓動時間。每次電腦重新開機時，Guard 會以指定的啓動模式來啓動。您可以選擇對電腦使用者指派不同角色 (兒童、青少年、成人)，以限制網際網路使用。您可以停用家長監護功能。

▶ 定義所需的家長監護設定，並按 [下一步]，繼續進行組態設定。

在接下來的 *[指派密碼]* 對話方塊中，您可以用密碼保護組態，避免未經授權的存取。如果您啓用了家長監護功能，特別建議使用此選項。

在接下來的 *[系統掃描]* 對話方塊中，您可以啓用或停用快速系統掃描。快速系統掃描可在組態完成後及電腦重新開機前進行，可掃描執行中的程式與最重要的系統檔案是否藏有病毒與惡意程式碼。

▶ 啓用或停用 *[快速系統掃描]* 選項，並按 *[下一步]* 繼續進行組態設定。

在接下來的對話方塊中，您可以按一下 *[完成]*，完成組態。

▶ 按一下 *[完成]* 完成組態。

隨即接受指定與選取的所有設定。

如果您已啓用 *[快速系統掃描]* 選項，[Luke Filewalker] 視窗隨即開啓。掃描程式會執行快速系統掃描。

繼續：快速安裝與使用者定義的安裝

如果您在安裝精靈結束時選取 **[重新啓動電腦]** 選項，電腦隨即重新開機。

在電腦重新啓動後，如果您已選取安裝精靈中的 **[顯示 Readme.txt]** 選項，讀我檔案隨即顯示。

安裝成功之後，建議您檢查控制中心中 *[概觀]::[狀態]* 下的程式是否爲最新版本。

- 必要時，執行更新以確保病毒定義檔是最新的。
- 接著執行完整系統掃描。

4.2 變更安裝

您可以針對目前的 AntiVir 城市安裝，選擇新增或移除個別程式元件 (請參閱下列章節：安裝與解除安裝::安裝模組)

如果您想要新增或移除目前安裝模組，可以使用 **Windows [控制台]** 中的 **[新增或移除程式]** 選項來**[變更/移除]** 相關程式。

選取 AntiVir 程式，並且按一下 **[變更]**]。在此程式的歡迎使用對話方塊中，選取 **[修改]** 選項。系統會引導您完成各項安裝變更。

4.3 安裝模組

在使用者定義的安裝或變更安裝中，您可以選取、新增或移除下列安裝模組。

– **Premium Security Suite**
此模組包含成功安裝 AntiVir 程式所需的所有元件。

– **AntiVir Guard**
AntiVir Guard 會在背景執行。在即時模式下，它會在開啓、寫入與複製等作業期間監視並修復檔案 (如果有需要的話)。每當使用者執行檔案操作 (例如，載入文件、執行、複製)，AntiVir 程式就會自動掃描檔案。重新命名檔案，不會造成 AntiVir Guard 觸發掃描作業。

– **AntiVir ProActive**
ProActiv 元件會監視應用程式動作，並在偵測到可疑的惡意程式碼應用程式行爲時，向使用者提出警示。此行爲式辨識模式可讓您防範不明的惡意程式碼。ProActive 元件是整合在 AntiVir Guard 之中。

– **AntiVir MailGuard**
MailGuard 是您的電腦與電子郵件伺服器之間的介面，後者可供您的電子郵件程式 (電子郵件用戶端) 下載電子郵件。連線的 MailGuard 可做爲電子郵件程式和電子郵件伺服器之間的 Proxy。所有內送的電子郵件都會透過這台 Proxy 來路由、掃描其中的病毒與有害程式，並轉寄給您的電子郵件程式。依據組態不同，程式會自動處理受影響的電子郵件或是要求使用者執行特定動作。此外，MailGuard 能可靠地保護您免於垃圾電子郵件的騷擾。

– **AntiVir WebGuard**
上網瀏覽時，您會使用網頁瀏覽器從網路伺服器要求資料。從網路伺服器傳輸的資料 (HTML 檔案、指令碼與圖片檔、Flash 檔案、影片與音樂串流等) 通常會直接存入瀏覽器快取以供網頁瀏覽器顯示，意味著 AntiVir Guard 無法執行即時掃描。如此一來，病毒與有害程式便可能存取您的電腦系統。WebGuard (即所謂的 HTTP Proxy) 可監視資料傳輸所使用的連接埠 (80、8080、3128) 並掃描傳輸的資料中是否有病毒與有害程式。依據組態不同，程式可能會自動處理受影響的檔案，或是提示使用者執行特定動作。

– **Avira FireWall**：
  Avira FireWall 可控制進出電腦的通訊。它會依據安全性原則允許或拒絕相關通訊活動。
– ***AntiVir Rootkit 保護***
  AntiVir Rootkit 保護會檢查您的電腦是否已安裝了某種特殊軟體，這類軟體一旦入侵電腦系統後，便無法再以傳統的惡意程式碼保護機制來偵測。
– **殼層延伸**
  ‘殼層延伸會在 [Windows 檔案總管] (滑鼠右鍵按鈕) 的內容功能表中產生一個項目 [以 AntiVir 掃描選取的檔案]。’透過這個項目，您可以直接掃描檔案或目錄。
– **備份**

備份元件可讓您手動與自動建立資料的鏡像備份。

4.4 解除安裝

如果希望從電腦移除 AntiVir 程式，您可以使用 **[新增或移除程式]** 以 **[變更/移除]** Windows [控制台] 中的程式。

若要解除安裝您的 AntiVir 程式 (例如，Windows XP 和 Windows Vista)：

▶ 經由 Windows **[開始]** 功能表，開啓 **[控制台]**。

▶ 按兩下 **[程式集]** (Windows XP：**[軟體]**)。

▶ 選取清單中的 AntiVir 程式，並按一下 **[移除]**。

系統會詢問您是否確定要移除程式。

▶ 按一下 **[是]** 確認。

系統會詢問您是否要重新啓用 Windows 防火牆 (會停用 Avira FireWall)。

▶ 按一下 **[是]** 確認。

這時所有程式元件都會移除。

▶ 按一下 **[完成]** 完成解除安裝。

必要時，會顯示對話方塊，建議您重新啓動電腦。

▶ 按一下 **[是]** 確認。

這時 AntiVir 程式已解除安裝，而且當您的電腦重新啓動時，程式的所有目錄、檔案與登錄項目都會一併刪除。

5 Premium Security Suite 概觀

本章包含 AntiVir 程式的功能與操作方式概觀。

– 請參閱下列章節：使用者介面與操作方式
– 請參閱下列章節：如何...?

5.1 使用者介面與操作方式

您可以經由三種程式介面元素來操作 AntiVir 程式：

– 控制中心：監控和控制 AntiVir 程式
– 組態：設定 AntiVir 程式
– 工作列的系統匣內的系統匣圖示：開啓控制中心和其他功能

5.1.1 控制中心

控制中心是專門設計來監視電腦系統的保護狀態，以及控制與操作 AntiVir 程式的保護元件與各項功能。



控制中心視窗分爲三個區域：**功能表列**、**瀏覽列**與詳細資料視窗**檢視**：

– **功能表列**：在控制中心功能表列中，您可以存取一般程式功能與此程式的相關資訊。
– **瀏覽區域**：在瀏覽區域中，您可以輕鬆切換個別的控制中心區段。這些個別的區段包含了程式元件的相關資訊與功能，並依據活動特性來排列瀏覽列。例如：活動 *[概觀]* - **[狀態]** 區段。

– **檢視:**此視窗會將選取的區段顯示在瀏覽區域中。依據區段而定，您可在詳細資料視窗上方列中，找到可執行各項功能與動作的按鈕。資料或資料物件會顯示在個別區段中的清單裡。您可以按一下方塊來定義清單排序方式，以排序清單。

啓動及關閉控制中心

若要啓動控制中心，可使用下列選項：

– 按兩下桌面上的程式圖示

– 經由 [開始] | [程式集] 功能表中的程式項目。

– 經由 AntiVir 程式的 [系統匣圖示]。

經由 **[檔案]** 功能表中的 **[關閉]** 功能表命令，或是按一下控制中心中的關閉索引標籤，關閉控制中心。

操作控制中心

若要瀏覽控制中心

▶ 在瀏覽列中選取一項活動。

此活動會開啓，並顯示其他區段。會選取活動的第一個區段，並顯示在檢視中。

▶ 必要時，按一下另一個區段將其顯示在詳細資料視窗中。

- 或 -

▶ 經由 *[檢視]* 功能表選取區段。

注意
您可以藉由 [ALT] 鍵，在功能表列中啓用鍵盤瀏覽功能。瀏覽功能一經啓用，您就可以使用方向鍵在功能表中移動。您可以使用 Return 鍵來啓用作用中的功能表項目。
若要開啓或關閉控制中心中的功能表，或是在各個功能表之間瀏覽，您還可以使用下列按鍵組合：[Alt] + 功能表中含底線的字母或功能表命令。如果您想要存取功能表、功能表命令或是子功能表，請按住 [Alt] 按鍵。

若要處理詳細資料視窗中顯示的資料或物件：

▶ 反白您希望編輯的資料或物件。

若要反白多項元素 (欄中的元素)，按住 Ctrl 按鍵或 Shift 按鍵不放並同時選取元素。

▶ 按一下詳細資料視窗上方列中的適當按鈕來編輯物件。

控制中心概觀

– **概觀**：在 **[概觀]** 中，您可以找到所有可用來監視 AntiVir 程式功能的區段。

- **[狀態]** 區段可讓您概要了解哪一個程式模組目前爲作用中，並提供最近執行的更新資訊。您還可以藉此了解是否擁有有效的授權。
- [事件] 區段可讓您檢視由特定程式模組所產生的事件。
- [報告] 區段可讓您檢視所執行的動作結果。

– **本機保護**：在 **[本機保護]** 中，您可以找到用來檢查電腦系統上的檔案是否藏有病毒與惡意程式碼的元件。

- 掃描區段可讓您輕易地設定並啓動指定掃描。預先定義的設定檔可讓您搭配已經調整的標準選項來執行掃描。同理，您也可以依據個人需求並藉由手動選取 (未儲存) 或是藉由建立使用者定義的設定檔，來調整病毒與有害程式的掃描方式。
- Guard 區段會顯示已掃描檔案的相關資訊與其他統計資料 (可隨時重設)，並讓您存取報告檔案。您只需實際按一下按鈕，就可獲得有關偵測到的最新病毒或有害程式詳細資訊。

– **線上保護**：在 **[線上保護]** 中，您可以找到用來保護電腦系統免於網際網路上的病毒與惡意程式碼威脅，同時防範未授權之網路存取的元件。

- MailGuard 區段可顯示 MailGuard 所掃描的所有電子郵件及其屬性和其他統計資料。您也可以訓練反垃圾郵件篩選器，以排除電子郵件地址免於日後的惡意程式碼或垃圾郵件掃描作業。您也可以從 MailGuard 緩衝區刪除電子郵件。
- [WebGuard] 區段會顯示所掃描 URL 和偵測到病毒的相關資訊，以及其他統計資料，而此項資料可隨時重設，且報告檔的存取權也可啓用。您只需實際按一下按鈕，就可獲得有關偵測到的最新病毒或有害程式詳細資訊。
- FireWall 區段可讓您進行 Avira FireWall 的基本設定。此外，還會顯示目前的資料傳輸率以及正在使用網路連線的所有作用中應用程式。

– **管理**：在 **[管理]** 中，您可以找到用以隔離與管理可疑或受感染檔案，以及用以規劃重複性工作的相關工具。

- 隔離區區段內含所謂的隔離區管理員。此區段可集中放置已經遭到隔離的所有檔案或是您想要隔離的可疑檔案。也可以將選取的檔案透過電子郵件方式傳送至 Avira 惡意程式碼研究中心。
- 排程管理員區段可讓您設定排定的掃描與更新工作以及備份工作，並讓您調整或刪除現有工作。

– **工具**：在 **[工具]** 中，您會找到其他資料安全工具。

- 在備份區段，您可以輕鬆、快速地建立資料備份，並啓始備份工作。

5.1.2 組態

您可以在 [組態] 中定義 AntiVir 程式的設定。安裝完畢後，AntiVir 程式會採用標準設定進行設定，確保爲您的電腦系統提供最佳保護。不過，您可能需要依據電腦系統或是 AntiVir 程式的特定需求，調整程式的保護元件。



[組態] 會開啓對話方塊：您可以經由 [確定] 或 [套用] 按鈕來儲存組態設定、按一下 [取消] 按鈕來刪除設定，或是透過 [預設值] 按鈕來還原預設的組態設定。您可以在左側的瀏覽列中，選取個別的組態區段。

存取組態

您可以使用下列幾個選項來存取組態：

- 經由 Windows 控制台。
- 經由 Windows 資訊安全中心 (從 Windows XP Service Pack 2 開始提供)。
- 經由 AntiVir 程式的 [系統匣圖示]。
- 經由 控制中心中的其他功能 | 組態功能表項目。
- 經由 控制中心中的組態按鈕。

注意
如果您是經由控制中心中的 **[組態]** 按鈕來存取組態，請移至控制中心裡目前作用中的區段之組態登錄。您必須選取專家模式以選取個別的組態登錄。在此情況中，會出現一個要求您啓用專家模式的對話方塊。

組態作業

[組態] 視窗與 [Windows 檔案總管] 的瀏覽方式是相同的：

- ▶ 按一下樹狀結構中的項目，將此組態區段顯示在詳細資料視窗中。
- ▶ 按一下項目前方的加號以展開組態區段，並在樹狀結構中顯示組態子區段。
- ▶ 若要隱藏組態子區段，在展開的組態區段前方按一下減號。

注意
若要啓用或停用組態選項並使用按鈕，您還可以使用下列按鍵組合：[Alt] + 選項名稱或按鈕描述中含底線的字母。

注意
所有的組態區段只會顯示在專家模式中。請啓用專家模式以檢視所有組態區段。在啓用期間必須定義的密碼，可用來保護專家模式。

如果您想要確認組態設定：

▶ 按一下 **[確定]**。

組態視窗隨即關閉，並接受相關設定。

- 或 -

▶ 按一下 **[接受]**。

隨即套用所有設定。組態視窗會維持開啓狀態。

如果您想要直接結束組態而不確認設定：

▶ 按一下 **[取消]**。

組態視窗隨即關閉，並捨棄相關設定。

如果您想要將所有組態設定還原爲預設值：

▶ 按一下 **[還原預設值]**。

組態的所有設定會還原爲預設值。當您還原預設值時，會遺失所有修正與自訂項目。

組態選項概觀

以下爲可用的組態選項：

– **掃描程式**：指定掃描組態

掃描選項

偵測有所發現時採取的動作

檔案掃描選項

指定掃描例外

指定掃描啓發式掃毒

報告功能設定

– **Guard**：即時掃描組態

掃描選項

偵測有所發現時採取的動作

即時掃描例外

即時掃描啓發式掃毒

報告功能設定

– **MailGuard**：MailGuard 組態

掃描選項：對 POP3 帳戶、IMAP 帳戶、外寄電子郵件 (SMTP) 啓用監視

對惡意程式碼採取的動作

MailGuard 掃描啓發式掃毒

AntiBot 功能：允許的 SMTP 伺服器與電子郵件寄件者

MailGuard 掃描例外

快取組態、清空快取

反垃圾郵件訓練資料庫組態、清空訓練資料庫

傳送的電子郵件頁尾組態

報告功能設定

– **WebGuard**：WebGuard 組態

掃描選項、啓用與停用 WebGuard

偵測有所發現時採取的動作

封鎖存取：有害的檔案類型與 MIME 類型、已知有害 URL (惡意程式碼、網路釣魚等) 的網路篩選器

WebGuard 掃描例外：URL、檔案類型、MIME 類型

WebGuard 啓發式掃毒

家長監護功能：針對網際網路的使用，進行角色式篩選與角色式時間限制

報告功能設定

– **FireWall**：FireWall 組態

介面卡規則設定

使用者定義的應用程式規則設定

受信任供應商清單 (供應用程式進行網路存取的例外項目)

展開的設定：規則逾時、鎖定 Windows 主機檔案、停止 Windows 防火牆、通知

快顯設定 (應用程式進行網路存取的警示)

– **備份**：

備份元件設定 (增量備份、於備份期間掃描病毒)

例外：定義要儲存的檔案

報告功能設定

– **一般**：

延伸的指定與即時掃描類別

控制中心與組態的密碼保護存取

資訊安全：更新狀態顯示、完整的系統掃描狀態顯示、產品保護

WMI：啓用 WMI 支援

事件記錄組態

報告功能組態

使用的目錄設定

更新： 下載伺服器的連線組態、產品更新的安裝

偵測到惡意程式碼時的警示音組態

5.1.3 系統匣圖示

安裝完畢後，您會在工作列的系統匣中看到 AntiVir 程式系統匣圖示：

圖示	Description
	AntiVir Guard 已啓用，FireWall 也已啓用
	AntiVir Guard 已停用，FireWall 也已停用

系統匣圖示會顯示 Guard 和 FireWall 服務的狀態。

您可以經由系統匣圖示的內容功能表，快速存取 AntiVir 程式的核心功能。若要開啓內容功能表，請以滑鼠右鍵按一下系統匣圖示。

內容功能表中的項目

– **啓用 AntiVir Guard**：啓用或停用 AntiVir Guard。
– **啓用 AntiVir MailGuard**：啓用或停用 AntiVir MailGuard。
– **啓用 AntiVir WebGuard**：啓用或停用 AntiVir WebGuard。
– **FireWall**：
– 啓用 FireWall：啓用或停用 FireWall
– 封鎖所有流量：已啓用：除了傳輸給主機電腦系統 (本機主機/IP 127.0.0.1) 的流量之外，會封鎖所有資料傳輸流量。
– 啓用遊戲模式：啓用或停用模式：
已啓用：啓用時，會套用所有定義的介面卡與應用程式規則。未定義任何規則的應用程式可存取網路，而且不會開啓任何快顯視窗。
– **啓動 AntiVir**：開啓控制中心。
– **設定 AntiVir**：開啓組態
– **開始更新**：開始更新。
– 說明：會開啓線上說明。
– **關於 Premium Security Suite:**開啓包含 AntiVir 程式相關資訊的對話方塊：產品資訊、版本資訊、授權資訊。
– **瀏覽 Avira 網站**：開啓網際網路上的 Avira 入口網站。前提是您必須具備有效的網際網路連線。

5.2 如何…？

5.2.1 啓用產品

若要啓動您的 AntiVir 產品，您可以使用下列選項：

- 使用有效的完整授權來啓用

  若要使用完整授權來啓用此程式 ，您需要有效的啓用金鑰 (內含所購買的授權資料)。您會透過電子郵件收到我們寄發的啓用金鑰，或在產品包裝上找到印刷的金鑰。

- 使用評估授權來啓用

您可以使用自動產生的評估授權來啓用您的 AntiVir 程式，以便在一定的時間內測試 AntiVir 程式 的完整功能。

注意
如需啓用產品或取得測試授權，您需要作用中的網際網路連結。
如果無法建立與 Avira GmbH 伺服器的連線，請檢查使用的防火牆設定：啓用產品時，請使用 HTTP 通訊協定與連接埠 80 (網路通訊)，並搭配加密通訊協定 SSL 與連接埠 443 進行連線。確定您的防火牆沒有封鎖傳入與傳出的資料。首先檢查是否可以使用網頁瀏覽器來存取網頁。

下面內容說明如何啓動您的 AntiVir 程式：

若您尚未安裝 AntiVir 程式：

▶ 安裝您的 AntiVir 程式。

系統會在安裝期間，要求您選取啓用選項。

- *啓用產品*

= 使用有效的完整授權來啓用

- *測試產品*

= 使用評估授權來啓用

▶ 輸入啓用金鑰，使用完整授權來啓用。

▶ 按 **[下一步]**，確認選取的啓用程序。

▶ 必要時，輸入個人註冊資料並按 **[下一步]** 加以確認。

您的授權資料會顯示在下一個視窗中。您的 AntiVir 程式已經啓用。

▶ 請繼續安裝。

若您已經安裝 AntiVir 程式：

▶ 在 [控制中心] 中，選取功能表項目 **[說明] ::[授權管理]**。

授權精靈隨即開啓，供您選取啓用選項。接下來的產品啓用步驟與上述程序完全相同。

5.2.2 執行自動更新

若要在 AntiVir 排程管理員建立工作，以自動更新 AntiVir 程式：

▶ 在 [控制中心]，選取 **[管理] ::[排程管理員]**。

▶ 按一下 *[使用精靈建立新的工作]* 圖示。

[工作的名稱和描述] 對話方塊隨即顯示。

▶ 賦予工作一個名稱，並適當地提供描述。

▶ 按 **[下一步]**。

[工作類型] 對話方塊隨即顯示。

▶ 從清單選取 **[更新工作]**。

▶ 按 **[下一步]**。

[工作時間] 對話方塊隨即顯示。

▶ 選取更新時間：

- 立即
- 每天
- 每週
- 間隔
- 一次
- 登入

注意
我們建議您定期且經常進行更新。建議的更新間隔爲：2 小時.

▶ 必要時，請依據選取項目指定日期。

▶ 必要時，請選取額外的選項 (可用性需視工作類型而定)：

- **同時在建立網際網路連線時開始工作**

  除了定義的頻率之外，當連線至網際網路時，也會執行工作。

- **如果時間已過，重新執行工作**

  會執行過去在指定時間無法執行的工作，例如，因爲電腦關機而無法執行的工作。

▶ 按 **[下一步]**。

[選取顯示模式] 對話方塊隨即顯示。

▶ 選取工作視窗的顯示模式：

- **最小化**：僅限進度列
- **最大化**：整個工作視窗
- **隱藏**：無工作視窗

▶ 按一下 **[完成]**。

新建立的工作會在 **[管理] ::[掃描]** 區段的起始頁上顯示爲啓用狀態 (勾選標記)。

▶ 必要時，停用不要執行的工作。

使用下列圖示，進一步定義工作：

檢視工作屬性

修改工作

刪除工作

開始工作

停止工作

5.2.3 啓動手動更新

您可以透過各種選項來手動啓動更新：手動啓動更新之後，病毒定義檔與掃描引擎會隨時更新。只有當您已在組態中啓用 **[下載並自動安裝產品更新]** 選項 (於一般 :: 更新

若要開始手動更新 AntiVir 程式：

▶ 以滑鼠右鍵按一下工作列中的 AntiVir 系統匣圖示。

內容功能表隨即顯示。

▶ 選取 **[開始更新]**。

[更新程式] 對話方塊隨即顯示。

- 或 -

▶ 在 [控制中心]，選取 **[概觀] :: [狀態]** 區段。

▶ 在 *[上次更新]* 欄位中，按一下 **[開始更新]** 連結。

[更新程式] 對話方塊隨即顯示。

- 或 -

▶ 在 [控制中心] 的 **[更新]** 功能表中，選取 *[開始更新]* 功能表命令。

[更新程式] 對話方塊隨即顯示。

注意
我們建議您定期自動進行更新。建議的更新間隔爲：2 小時.

注意
您也可以直接透過 Windows 資訊安全中心，執行手動更新。

5.2.4 指定掃描：使用掃描設定檔來掃描病毒與惡意程式碼

掃描設定檔內含一組要掃描的磁碟機與目錄。

以下爲透過掃描設定檔來掃描時的可用選項：

– 當預先定義的掃描設定檔符合您的需求時，

使用預先定義的掃描設定檔。

– 當您想要使用自訂掃描設定檔來掃描時，

自訂並套用掃描設定檔 (手動選取)。

– 當您想要建立自己的掃描設定檔時，

建立並套用新的掃描設定檔。

依據作業系統不同，啓動掃描設定檔時可以使用的圖示也不同：

– Windows XP 與 Windows 2000：

此圖示會透過掃描設定檔啓動掃描。

– Windows Vista：

在 Microsoft Windows Vista 中，控制中心目前的權限有限，例如目錄與檔案的存取權限。在控制中心，您只能以延伸的系統管理員權限來執行特定動作與檔案存取。您必須在每次掃描開始時透過掃描設定檔來授予這些延伸的系統管理員權限。

此圖示會透過掃描設定檔啟動有限的掃描。只會掃描 Windows Vista 已授予存取權限的目錄與檔案。

此圖示會以延伸的系統管理員權限來啟動掃描。確認選取後，會針對選取的掃描設定檔掃描其中的所有目錄與檔案。

若要使用掃描設定檔來掃描病毒與惡意程式碼：

▶ 移至 [控制中心] 並選取 **[本機保護] ::[掃描]**。

預先定義的掃描設定檔隨即顯示。

▶ 選取其中一項預先定義的掃描設定檔。

-或-

▶ 調整掃描設定檔 *[手動選取]*。

-或-

▶ 建立新的掃描設定檔

▶ 按一下圖示 (Windows XP： 或 Windows Vista：).

▶ *[Luke Filewalker]* 視窗隨即顯示，並開始進行指定掃描。

掃描完成時，會顯示結果。

如果您想要調整掃描設定檔：

▶ 在掃描設定檔中，展開 **[手動選取]** 檔案樹狀結構，以開啓所有要掃描的磁碟機與目錄。

- 按一下 **+** 圖示：下一個目錄層級隨即顯示。
- 按一下 **-** 圖示：下一個目錄層級隨即隱藏。

▶ 按一下適當目錄層級的相關方塊，反白您要掃描的節點和目錄。

以下爲可用來選取目錄的選項：

- 目錄，包括子目錄 (黑色勾選標記)
- 目錄，不包括子目錄 (綠色勾選標記)
- 僅限單一目錄的子目錄 (灰色勾選標記，子目錄是黑色勾選標記)
- 無目錄 (無勾選標記)

如果您想要建立新的掃描設定檔：

▶ 按一下 **[建立新的設定檔]** 圖示。

[新的設定檔] 設定檔會顯示在先前建立的設定檔下方。

▶ 必要時，按一下 圖示，重新命名掃描設定檔。

▶ 按一下個別的目錄層級核取方塊，反白要儲存的節點與目錄。

以下爲可用來選取目錄的選項：

- 目錄，包括子目錄 (黑色勾選標記)
- 目錄，不包括子目錄 (綠色勾選標記)
- 僅限單一目錄的子目錄 (灰色勾選標記，子目錄是黑色勾選標記)
- 無目錄 (無勾選標記)

5.2.5 指定掃描：使用拖放方式掃描病毒與惡意程式碼

若要使用拖放方式，有系統地掃描病毒與惡意程式碼：

AntiVir 程式的控制中心已經開啓。

▶ 反白您要掃描的檔案或目錄。

▶ 使用滑鼠左鍵將反白的檔案或目錄拖曳至 *[控制中心]*。

[Luke Filewalker] 視窗隨即顯示，並開始進行指定掃描。

掃描完成時，會顯示結果。

5.2.6 指定掃描：透過內容功能表來掃描病毒與惡意程式碼

若要透過內容功能表，有系統地掃描病毒與惡意程式碼：

▶ 在您要掃描的檔案或目錄上，按一下滑鼠右鍵 (例如，在 [Windows 檔案總管] 中、在桌面上，或是在開啓的 Windows 目錄)。

[Windows 檔案總管] 內容功能表隨即顯示。

▶ 選取內容功能表中的 **[以 AntiVir 掃描選取的檔案]**。

[Luke Filewalker] 視窗隨即顯示，並開始進行指定掃描。

掃描完成時，會顯示結果。

5.2.7 指定掃描：自動掃描病毒與惡意程式碼

注意
安裝後，會在排程管理員中建立 *[完整系統掃描]* 的掃描工作：完整的系統掃描會依據建議間隔自動執行。

若要建立工作以自動掃描病毒與惡意程式碼：

▶ 在 [控制中心]，選取 **[管理] :: [排程管理員]**。

▶ 按一下 圖示。

[工作的名稱和描述] 對話方塊隨即顯示。

▶ 賦予工作一個名稱，並適當地提供描述。

▶ 按 **[下一步]**。

[工作類型] 對話方塊隨即顯示。

▶ 選取 **[掃描工作]**。

▶ 按 **[下一步]**。

[選取設定檔] 對話方塊隨即顯示。

▶ 選取要掃描的設定檔。

▶ 按 **[下一步]**。

[工作時間] 對話方塊隨即顯示。

▶ 選取掃描時間：

- **立即**
- **每天**
- **每週**
- **間隔**
- **一次**
- **登入**

▶ 必要時，請依據選取項目指定日期。

▶ 必要時，請選取下列額外的選項 (可用性需視工作類型而定)：

- **如果時間已過，重新執行工作**

  會執行過去在指定時間無法執行的工作，例如，因為電腦關機而無法執行的工作。

▶ 按 **[下一步]**。

[選取顯示模式] 對話方塊隨即顯示。

▶ 選取工作視窗的顯示模式：

- **最小化**：僅限進度列
- **最大化**：整個工作視窗
- **隱藏**：無工作視窗

▶ 如果您要在完成掃描時自動關閉電腦，請選取 *[關閉電腦]* 選項。只有當顯示模式設為最小化或最大化時，才能使用此選項。

▶ 按一下 **[完成]**。

新建立的工作會在 *[管理 ::[排程管理員]* 區段的起始頁上顯示為啓用狀態 (勾選標記)。

▶ 必要時，停用不要執行的工作。

使用下列圖示，進一步定義工作：

檢視工作屬性

修改工作

刪除工作

開始工作

停止工作

5.2.8 指定掃描：Rootkit 和作用中的惡意程式碼指定掃描

若要掃描作用中的 Rootkit，請使用預先定義的掃描設定檔 *[掃描 Rootkit 和作用中的惡意程式碼]*。

若要有系統地掃描作用中的 Rootkit：

▶ 移至 [控制中心] 並選取 **[本機保護] ::[掃描程式]**。

預先定義的掃描設定檔隨即顯示。

▶ 選取預先定義的掃描設定檔 **[掃描 Rootkit 和作用中的惡意程式碼]**。

▶ 必要時，按一下目錄層級核取方塊，反白要掃描的其他節點與目錄。

▶ 按一下圖示 (Windows XP： 或 Windows Vista：).

[Luke Filewalker] 視窗隨即顯示，並開始進行指定掃描。

掃描完成時，會顯示結果。

5.2.9 回應偵測到的病毒與惡意程式碼

針對 AntiVir 程式的個別保護元件，您可以在 [組態] 的 *[偵測有所發現時採取的動作]* 區段底下，定義 AntiVir 程式對偵測到的病毒或有害程式的回應方式。

Guard 的 ProActive 元件也沒有可設定的動作選項：偵測通知一律顯示在 *[Guard]:[可疑的應用程式行為]* 視窗。

掃描程式的動作選項：

– **互動式**

在互動式動作模式中，掃描程式的掃描結果會顯示在對話方塊中。此選項會啓用爲預設值。
如果使用**掃描程式掃描**，在掃描結束時，您會收到一則警示，內含受影響的檔案清單。您可以使用即時線上功能表，針對各種受感染的檔案選取要執行的動作。您可以針對所有受感染的檔案執行標準動作，或是取消掃描程式。

– **自動**

在自動動作模式中，當偵測到病毒或有害程式時，您在此區域選取的動作會自動執行。

Guard 的動作選項：

– **互動式**

在互動式動作模式中，會拒絕資料存取並顯示桌面通知。在桌面通知中，您可以移除偵測到的惡意程式碼，或使用 [詳細資料] 按鈕將惡意程式碼傳送至掃描程式元件，執行進一步病毒管理。掃描程式會開啓含有偵測通知的視窗，提供您透過內容功能表管理受影響檔案的各種選項 (請參閱偵測::掃描程式)：

– **自動**

在自動動作模式中，當偵測到病毒或有害程式時，您在此區域選取的動作會自動執行。

MailGuard、WebGuard 的動作選項：

– **互動式**

在互動式動作模式中，一旦偵測到病毒或有害程式，會出現對話方塊供您針對感染的物件選取處理方式。此選項會啓用爲預設值。

– **自動**

在自動動作模式中，當偵測到病毒或有害程式時，您在此區域選取的動作會自動執行。

在互動式動作模式中，您可以從警示中選取受感染物件適用的動作，並按一下 [確認] 來執行選取的動作，藉此回應偵測到的病毒與有害程式。

您可以選取下列動作來處理感染的物件：

注意
可使用的動作取決於作業系統、負責報告偵測的保護元件 (AntiVir Guard、AntiVir 掃描程式、AntiVir MailGuard、AntiVir WebGuard)，以及偵測到的惡意程式碼類型。

掃描程式和 Guard **的動作 (而不是 ProActiv 偵測)：**

– **修復**

檔案已修復。

只有當受感染的檔案可以修復時，才能使用此選項。

– **移至隔離區**

檔案會封裝爲特殊格式 (**.qua*) 並移至硬碟上的隔離區目錄 *INFECTED*，這樣就無法再直接存取。 稍後可以在隔離區中修復此目錄中的檔案，必要時也可傳送至 Avira GmbH。

– **刪除**

檔案將會刪除。此處理序在速度上會比 *[覆寫並刪除]* 要來得快速。如果偵測到開機磁區病毒，可以刪除開機磁區來加以刪除。會寫入新的開機磁區。

– **覆寫並刪除**

此檔案會以預設範本模式來覆寫，然後刪除。此檔案無法還原。

– **重新命名**

此檔案會重新命名爲 **.vir* 副檔名。如此將無法再直接存取這些檔案 (例如按兩下滑鼠)。檔案可以在之後修復並重新賦予其原始名稱。

– **略過**

不需要採取進一步動作。受感染的檔案仍會在電腦上繼續運作。

警告
這樣可能會導致資料遺失，並對作業系統造成傷害！請僅在例外情況下才選取 *[略過]* 選項。

– **一律忽略**

Guard 偵測到狀況時的動作選項：Guard 未執行其他動作。允許存取檔案。直到電腦重新啓動或該病毒定義檔更新爲止，允許對此檔案進行其他存取，並且不會提供任何其他通知。

– **複製至隔離區**

偵測到 Rootkit 時的動作選項：偵測項目會複製至隔離區。

– **修復開機磁區 | 下載修復工具**

偵測到受感染開機磁區時的動作選項：可使用一些修復受感染磁碟機的選項。如果 AntiVir 程式無法執行修復，您可以下載用於偵測及移除開機磁區病毒的特殊工具。

注意
如果您對執行中的處理序執行動作，有問題的處理序會先終止，然後執行動作。

ProActiv 元件偵測到狀況時 **Guard** 的動作 **(**應用程式有可疑行爲動作的通知**)**：

– 信任的程式

應用程式會繼續執行。程式已加入許可的應用程式清單中，ProActive 元件不會監視此程式。加入至許可的應用程式清單時，監視類型會設爲 *[*內容*]*。這表示檔案內容保持不變時，ProActive 元件才不會監視應用程式 (請參閱組態 ::Guard::ProActive::應用程式篩選器:許可的應用程式)。

– 封鎖程式一次

會封鎖應用程式 (即終止應用程式)。應用程式的動作持續受到 ProActive 元件監視。

– 永遠封鎖此程式

會封鎖應用程式 (即終止應用程式)。程式已加入封鎖的應用程式清單中，無法再執行 (請參閱組態::Guard::ProActive::應用程式篩選器:要封鎖的應用程式)。

– 略過

應用程式會繼續執行。應用程式的動作持續受到 ProActive 元件監視。

MailGuard 動作：內送電子郵件

– 移至隔離區

電子郵件 (包括所有附件) 會移至隔離區。受影響的電子郵件會刪除。電子郵件本文和所有附件都會以預設內容來取代。

– 刪除

受影響的電子郵件會刪除。電子郵件本文和所有附件都會以預設內容來取代。

– 刪除附件

受感染的附件會以預設內容來取代。如果電子郵件本文受到影響，會加以刪除並同時以預設內容來取代。電子郵件本身會遞送出去。

– 將附件移至隔離區

受感染的附件會放置到隔離區並加以刪除 (以預設內容來取代)。電子郵件本文會遞送出去。受影響的附件稍後可由隔離區管理員來遞送。

– 略過

受影響的電子郵件會遞送出去。

警告
如此一來，病毒與有害程式便可能存取您的電腦系統。請僅在例外情況下才選取 **[**略過**]** 選項。請停用郵件用戶端中的預覽功能，而且絕對不要按兩下附件加以開啓！

MailGuard 動作：外寄電子郵件

– 將郵件移至隔離區 **(**不要傳送**)**

會將電子郵件 (包括所有附件) 複製到隔離區，而且不會傳送出去。電子郵件會留在您的電子郵件用戶端寄件匣中。您的電子郵件程式會出現錯誤訊息。來自您電子郵件帳戶的其他所有電子郵件，都會接受惡意程式碼掃描。

– **封鎖郵件的傳送 (不要傳送)**

電子郵件不會傳送出去，並會留在您的電子郵件用戶端寄件匣中。您的電子郵件程式會出現錯誤訊息。來自您電子郵件帳戶的其他所有電子郵件，都會接受惡意程式碼掃描。

– **略過**

受影響的電子郵件會傳送出去。

警告
病毒與有害程式可以藉由這種方式，入侵電子郵件收件者的電腦系統。

WebGuard 動作：

– **拒絕存取**

網路伺服器要求的網站與/或傳輸的任何資料或檔案，都不會傳送到您的網頁瀏覽器。網頁瀏覽器上會顯示一則錯誤訊息，通知您已經拒絕存取。

– **移至隔離區**

網路伺服器要求的網站與/或傳輸的任何資料或檔案，都會移至隔離區。如果受影響的檔案具有參考價值，可以從隔離區管理員復原，或在必要時將其傳送至 Avira 惡意程式碼研究中心。

– **略過**

WebGuard 會將網路伺服器要求的網站與/或傳輸的資料與檔案，傳送到您的網頁瀏覽器。

警告
如此一來，病毒與有害程式便可能存取您的電腦系統。請僅在例外情況下才選取 **[略過]** 選項。

注意
建議您將任何無法修復的可疑檔案移至隔離區。

注意
您也可以將啓發式掃毒所報告的檔案傳送給我們進行分析。
例如，您可以將這些檔案上傳到我們的網站：http://www.avira.tw/sample-upload
您可以從指定的檔名前置詞 (*HEUR/* 或 *HEURISTIC/*) 來識別啓發式掃毒報告的檔案，例如：*HEUR/testfile.**。

5.2.10 隔離區：處理隔離區檔案 (*.qua)

若要處理隔離區檔案：

- 在 [控制中心]，選取 **[管理] ::[隔離區]** 區段。
- 檢查哪些檔案受到影響，必要時，可以從其他位置將原始檔案重新載入至電腦。

如果您想要了解檔案詳細資訊：

- 反白檔案，然後按一下 。

  [屬性] 對話方塊隨即顯示，內含檔案的詳細資訊。

如果您想要重新掃描檔案：

如果 AntiVir 程式病毒定義檔已經更新，並懷疑報告為誤判情況時，建議您掃描檔案。您可以藉由重新掃描來確認遭到誤判的檔案，然後還原該檔案。

- 反白檔案，然後按一下 。

  您可以使用指定掃描設定，掃描檔案中是否有病毒與惡意程式碼。

  掃描完畢後會顯示 *[掃描統計資料]* 對話方塊，內含重新掃描前後的檔案狀態統計資料。

若要刪除檔案：

- 反白檔案，然後按一下 。

如果您要將檔案上傳至 Avira 惡意程式碼研究中心網路伺服器，進行分析：

- 反白您要上傳的檔案。
- 按一下 圖示。

  這時會開啓內含表單的對話方塊，供您輸入連絡資料。

- 請輸入所有必要的資料。
- 選取類型：**可疑的檔案**或**誤判**。
- 按一下 **[確定]**。

  檔案隨即以壓縮形式上傳至 Avira 惡意程式碼研究中心網路伺服器。

注意
在下列情況中，建議交由 Avira 惡意程式碼研究中心進行分析：
啓發式掃毒目標 (可疑的檔案)：在掃描期間，某一檔案經由 AntiVir 程式歸類為可疑，並移至隔離區：病毒偵測對話方塊或是掃描產生的報告檔案已建議將檔案交由 Avira 惡意程式碼研究中心進行分析。
可疑的檔案：您將視為可疑的檔案移至隔離區，但是針對檔案進行的病毒與惡意程式碼掃描結果卻沒問題。
誤判：您假定病毒偵測結果為誤判：AntiVir 程式針對不太可能遭到惡意程式碼感染的檔案回報偵測到可疑項目。

注意
上傳的檔案大小上限為 20 MB (未壓縮) 或 8 MB (壓縮)。

注意
您一次只能上傳一個檔案。

如果您要從隔離區將隔離區物件複製到另一個目錄：

- 反白隔離區物件，然後按一下 。

  掃描對話方塊隨即開啓，供您選取目錄。

- 選取您要儲存隔離區物件複本的目錄，並確認選擇。

  選取的隔離區物件會儲存到選取的目錄。

注意
隔離區物件不同於還原的檔案。隔離區物件已加密，無法以其原始格式執行或讀取。

如果您要將隔離區物件的屬性匯出在文字檔中：

▶ 反白隔離區物件，然後按一下 。

文字檔會開啓，其中包含選取的隔離區物件資料。

▶ 儲存文字檔。

您也可以還原隔離區的檔案：

– 請參閱下列章節：隔離區：還原隔離區的檔案

5.2.11 隔離區：還原隔離區的檔案

不同的作業系統，會以不同的圖示來控制還原程序：

– Windows XP 與 Windows 2000：

此圖示可將檔案還原至原始目錄。

此圖示可將檔案還原至自選的目錄。

– Windows Vista：

在 Microsoft Windows Vista 中，控制中心目前的權限有限，例如目錄與檔案的存取權限。在控制中心，您只能以延伸的系統管理員權限來執行特定動作與檔案存取。您必須在每次掃描開始時透過掃描設定檔來授予這些延伸的系統管理員權限。

此圖示可將檔案還原至自選的目錄。

此圖示可將檔案還原至原始目錄。如果需要透過延伸的系統管理員權限來存取此目錄，系統會顯示對應的要求。

若要還原隔離區的檔案：

警告
這樣可能會導致資料遺失，並對電腦作業系統造成傷害！請僅在例外情況下，才使用 *[還原選取的物件]* 功能。請在全新的掃描能夠修復檔案時，才加以還原。

重新掃描與修復的檔案。

▶ 在 [控制中心]，選取 **[管理] ::[隔離區]** 區段。

注意
當檔案副檔名爲 **.eml* 時，電子郵件和電子郵件附件只能用選項 還原。

若要將檔案還原至原始位置：

▶ 反白檔案，然後按一下圖示 (Windows 2000/XP： 、Windows Vista)。
電子郵件不適用此選項。

注意

當檔案副檔名為 **.eml* 時，電子郵件和電子郵件附件只能用選項 還原。

會顯示一則訊息，詢問您是否要還原檔案。

▶ 按一下 **[是]**。

檔案會還原至當初尚未移至隔離區之前的所在目錄。

若要將檔案還原至指定目錄：

▶ 反白檔案，然後按一下 。

會顯示一則訊息，詢問您是否要還原檔案。

▶ 按一下 **[是]**。

會顯示 Windows 預設視窗供您選取目錄。

▶ 請選取要還原檔案的目錄，並確認選取。

檔案會還原至選取的目錄。

5.2.12 隔離區：將可疑的檔案移至隔離區

若要將可疑的檔案手動移至隔離區：

▶ 在 [控制中心]，選取 **[管理] :: [隔離區]** 區段。

▶ 按一下 圖示。

會顯示 Windows 預設視窗供您選取檔案。

▶ 請選取檔案並確認。

這時檔案已移至隔離區。

您可以使用 AntiVir 掃描程式來掃描隔離區的檔案：

- 請參閱下列章節：隔離區：處理隔離區檔案 (*.qua)

5.2.13 掃描設定檔:修訂或刪除掃描設定檔中的檔案類型

若要指定要掃描的額外檔案類型，或是從掃描設定檔中排除特定檔案類型 (只能透過手動選取與自訂的掃描設定檔)：

在 [控制中心]，移至 **[本機保護] ::** *[掃描]* 區段。

▶ 請以滑鼠右鍵按一下您要編輯的掃描設定檔。

內容功能表隨即顯示。

▶ 選取 **[檔案篩選器]**。

▶ 按一下內容功能表右側的小三角形，進一步展開內容功能表。

[預設值]、*[掃描所有檔案]* 與 *[使用者定義]* 項目隨即顯示。

▶ 選取 **[使用者定義]**。

[副檔名] 對話方塊隨即顯示，內含此掃描設定檔要掃描的所有檔案類型清單。

如果您想要從掃描中排除某個檔案類型：

▶ 反白檔案類型，然後按一下 **[刪除]**。

如果您想要將某個檔案類型新增至掃描：

- 反白檔案類型。
- 按一下 **[新增]** 並在輸入方塊中輸入檔案類型的副檔名。

  最多可接受 10 個字元，而且不可在字元之前輸入句點。可以使用萬用字元 (* 與 ?) 來取代相關字元。

5.2.14 掃描設定檔:爲掃描設定檔建立桌面捷徑

您可以直接透過桌面的掃描設定檔捷徑來啓動指定掃描，無須存取 AntiVir 程式'控制中心。

若要爲掃描設定檔建立桌面捷徑：

在 [控制中心]，移至 **[本機保護] ::***[掃描]* 區段。

- 選取您要建立捷徑的掃描設定檔。
- 按一下 圖示。

  立即建立桌面捷徑。

5.2.15 事件：篩選事件

AntiVir 程式元件所產生的事件會顯示在控制中心的 **[概觀::事件]** 底下 (類似於您的 Windows 作業系統的事件顯示)。這些程式元件如下：

- 更新程式
- 排程管理員
- Guard
- MailGuard
- 掃描程式
- FireWall
- WebGuard
- 備份
- 協助程式服務
- ProActive

會顯示下列事件類型：

- 資訊
- 警告
- 錯誤
- 偵測的發現

若要篩選顯示的事件：

- 在 [控制中心]，選取 **[概觀] ::**活動。
- 勾選程式元件方塊，顯示啓用的元件事件。

  \- 或 -

  取消勾選程式元件方塊，隱藏停用的元件事件。

- 勾選事件類型方塊以顯示這些事件。

  - 或 -

  取消勾選事件類型方塊以隱藏這些事件。

5.2.16 MailGuard：排除不要掃描的電子郵件地址

若要定義將哪些電子郵件地址 (寄件者) 從 MailGuard 掃描中排除 (加入白名單)：

- 移至 [控制中心] 並選取 **[線上保護::[MailGuard]**。

  此名單會顯示內送的電子郵件。

- 反白您要從 MailGuard 掃描中排除的電子郵件。
- 按一下適當的圖示，從 MailGuard 掃描中排除電子郵件：

  未來將不再掃描選取的電子郵件地址來檢查病毒與有害的程式。

  未來將不再掃描選取的電子郵件地址來尋找垃圾郵件。

會將電子郵件寄件者地址包含在排除清單中，未來將不再掃描其中是否含有病毒、惡意程式碼或垃圾郵件。

警告
僅從 MailGuard 掃描中排除可以完全信任的寄件者電子郵件地址。

注意
在[控制中心] 的 [MailGuard] ::[一般] ::[例外] 底下，您可以將其他的電子郵件地址新增到排除清單中，或是從排除清單中移除電子郵件地址。

5.2.17 MailGuard：訓練反垃圾郵件模組

反垃圾郵件模組內含訓練資料庫。您的個別分類準則會記錄在此訓練資料庫中。經過一段時間後，調整過的內部篩選器、演算法與垃圾郵件評估準則將合乎您的個人準則要求。

若要針對訓練資料庫分類電子郵件：

- 移至 [控制中心]，並選取區段 **[線上保護] ::[MailGuard]**。

  此名單會顯示內送的電子郵件。

- 反白您要分類的電子郵件。
- 按一下適當的圖示，將電子郵件識別爲垃圾郵件或有用的郵件，亦即「良好的」電子郵件。

  電子郵件會輸入至訓練資料庫，並套用至下一個垃圾郵件識別處理序。

注意
您可以在組態的 [MailGuard::[一般] ::反垃圾郵件] 中刪除此訓練資料庫。

5.2.18 FireWall：選取 FireWall的安全性等級

有各種安全性等級可供選擇。依據選擇的等級，您可以搭配不同的介面卡規則組態選項。

以下為可用的安全性等級：

– **低**
- 會偵測到洪水攻擊和連接埠掃描。

– **中**
- 會捨棄可疑的 TCP 和 UDP 封包。
- 可預防洪水攻擊和連接埠掃描。

– **高**
- 電腦不會在網路上顯示出來。
- 會封鎖所有外部連線。
- 可預防洪水攻擊和連接埠掃描。

– **使用者**
- 使用者定義的規則：一旦選取此安全性等級，程式會自動識別已經修改的介面卡規則。

注意
所有預先定義之 Avira FireWall 規則的預設安全性等級設定都是 **[高]**

若要定義 FireWall 的安全性等級：

▶ 移至 [控制中心] 並選取 **[線上保護 :: FireWall]**。

▶ 將滑桿移至所需的安全性等級。

選取的安全性等級會立即套用。

5.2.19 備份：手動建立備份

控制中心中的備份工具可讓您輕鬆、快速地備份個人資料。在 [Avira 備份] 中，您可以建立所謂的鏡像備份，以便使用最少的資源來儲存最近的資料。[Avira 備份] 可讓您在備份程序期間掃描資料中的病毒與惡意程式碼。檔案只要受到感染，就不會儲存起來。

注意
不同於版本備份的是，鏡像備份並不會儲存個別的備份版本。鏡像備份內含上次備份時的資料庫存。不過，如果儲存在資料庫存中的檔案已經刪除，後來的備份作業就不會進行任何比對動作，亦即備份中仍舊會存在刪除的檔案。

注意
使用 [Avira 備份] 預設值時，只會儲存修改的檔案，並會掃描檔案中的病毒與惡意程式碼。您可以在組態的 [備份::設定] 底下變更這些設定。

若要使用備份工具來儲存資料：

▶ 在 [控制中心] 選取 **[工具]::[備份]** 區段。

預設的備份設定檔隨即顯示。

▶ 選取其中一項預設的備份設定檔。

-或-

▶ 調整備份設定檔 *[手動選取]*。

-或-

▶ 建立新的備份設定檔

▶ 請在 *[目的地目錄]* 方塊中，針對選取的設定檔輸入儲存位置。

備份的儲存位置可以是電腦、連線的網路磁碟機或是卸除式磁碟 (例如 USB 隨身碟或磁碟片) 上的目錄。

▶ 按一下 圖示。

[Avira 備份] 視窗隨即顯示，並開始備份。備份的狀態與結果會顯示在備份視窗中。

如果您想要修改備份設定檔：

▶ 在掃描設定檔中，展開 *[手動選取]* 檔案樹狀結構，以開啟所有要儲存的磁碟機與目錄：

- 按一下 + 圖示：下一個目錄層級隨即顯示。
- 按一下 - 圖示：下一個目錄層級隨即隱藏。

▶ 按一下個別的目錄層級方塊，反白要儲存的節點與目錄：

以下為可用來選取目錄的選項：

- 目錄，包括子目錄 (黑色勾選標記)
- 目錄，不包括子目錄 (綠色勾選標記)
- 僅限單一目錄的子目錄 (灰色勾選標記，子目錄是黑色勾選標記)
- 無目錄 (無勾選標記)

如果您想要建立新的備份設定檔：

▶ 按一下 **[建立新的設定檔]** 圖示。

[新的設定檔] 設定檔會顯示在先前建立的設定檔下方。

▶ 必要時，按一下 圖示，賦予備份設定檔一個名稱。

▶ 按一下個別目錄層級的核取方塊，反白要儲存的節點與目錄。

以下為可用來選取目錄的選項：

- 目錄，包括子目錄 (黑色勾選標記)
- 目錄，不包括子目錄 (綠色勾選標記)
- 僅限單一目錄的子目錄 (灰色勾選標記，子目錄是黑色勾選標記)
- 無目錄 (無勾選標記)

5.2.20 備份：建立自動資料備份

本節將說明如何啓始工作來建立自動資料備份：

▶ 在 [控制中心] 中選取 **[管理]::[排程管理員]** 區段。

▶ 按一下 圖示。

[工作的名稱和描述] 對話方塊隨即顯示。

- 賦予工作一個名稱，並適當地提供描述。
- 按 **[下一步]**。

[工作類型] 對話方塊隨即顯示。

- 選取 **[備份工作]**。
- 按 **[下一步]**。

[選取設定檔] 對話方塊隨即顯示。

- 選取要掃描的設定檔。

注意
只會顯示已經指定儲存位置的備份設定檔。

- 按 **[下一步]**。

[工作時間] 對話方塊隨即顯示。

- 選取掃描時間：
  - 立即
  - 每天
  - 每週
  - 間隔
  - 一次
  - 登入
  - 隨插即用

  如果選取做為備份設定檔儲存位置的卸除式磁碟已連線至電腦，則系統一律會建立「隨插即用」事件備份。若要啓用「隨插即用」備份事件，需要輸入 USB 隨身碟做為儲存位置。

- 必要時，請依據選取項目指定日期。
- 必要時，請選取下列額外的選項 (可用性需視工作類型而定)：
  - **如果時間已過，重新執行工作**

  會執行過去在指定時間無法執行的工作，例如，因為電腦關機而無法執行的工作。

- 按 **[下一步]**。

[選取顯示模式] 對話方塊隨即顯示。

- 選取工作視窗的顯示模式：
  - **最小化**：僅限進度列
  - **最大化**：整個備份視窗
  - **隱藏**：無備份視窗
- 按一下 **[完成]**。

新建立的工作會在 *[管理] ::[排程管理員]* 區段的起始頁上顯示為啓用狀態 (勾選標記)。

- 必要時，停用不要執行的工作。

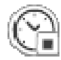
使用下列圖示，進一步定義工作：

 檢視工作屬性

 修改工作

 刪除工作

 開始工作

 停止工作

6 掃描程式

有了掃描程式元件，您可以針對病毒與有害程式執行鎖定掃描 (指定掃描)。以下爲掃描受感染檔案時的可用選項：

– **經由內容功能表進行指定掃描**
  例如，當您希望掃描個別檔案與目錄時，建議您透過內容功能表執行指定掃描 (滑鼠右鍵的 **[以 AntiVir 掃描選取的檔案]** 項目)。透過內容功能表來執行指定掃描的另一項優勢，則是不需要先啓動 控制中心。

– **經由拖放方式進行指定掃描**
  當您將檔案或目錄拖放到 控制中心 的程式視窗中時，掃描程式會掃描檔案或目錄與其下的所有子目錄。例如，當您希望掃描儲存在桌面上的個別檔案與目錄時，建議您使用此程序進行。

– 經由設定檔進行指定掃描
  當您希望定期掃描特定目錄與磁碟機時 (例如，您經常在其中儲存新檔案的工作目錄或磁碟機)，建議您使用此程序進行。如此一來，您不需要針對每個全新的掃描作業重複選取相關目錄與磁碟機，只要選取使用的相關設定檔即可。

– **經由排程管理員進行指定掃描**
  排程管理員可讓您執行有時效的掃描作業。

若要掃描 Rootkit、開機磁區病毒與作用中的處理序時，就需要特殊的程序。以下爲可用的選項：

– 透過掃描設定檔 *[掃描 Rootkit 和作用中的惡意程式碼]* 掃描 Rootkit
– 經由掃描設定檔 **[作用中處理序]** 來掃描作用中的處理序
– 經由 **[其他功能]** 功能表中的 **[掃描開機磁區病毒]** 功能表命令來掃描開機磁區病毒

7 更新

防毒軟體的有效性取決於程式是否為最新狀態，特別是病毒定義檔與掃描引擎。為了執行定期更新，我們已將更新程式元件整合在 AntiVir 中。更新程式可確保 AntiVir 程式保持在最新狀態，而且有能力處理隨時出現的全新病毒。更新程式會更新下列元件：

– 病毒定義檔：

病毒定義檔內含 AntiVir 程式掃描病毒與惡意程式碼並修復受感染物件時所用的有害程式病毒模式。

– 掃描引擎：

掃描引擎內含 AntiVir 程式用來掃描病毒與惡意程式碼的方法。

– 程式檔案 (產品更新)：

產品更新的更新套件可為個別程式元件提供額外的功能。

更新會檢查病毒定義檔與掃描引擎是否為最新，必要時還會實作更新。依據組態設定，更新程式還會執行產品更新，或是通知您可用的產品更新。在產品更新後，您可能必須重新啓動電腦系統。如果只更新病毒定義檔與掃描引擎，電腦不必重新啓動。

注意
為了安全起見，更新程式會檢查電腦中的 Windows 主機檔案是否遭到竄改。舉例來說，惡意程式碼可以藉由這種方式操控更新 URL，使得更新程式被導向至有害的下載網站。一旦發生 Windows 主機檔案遭到竄改的情形，便會顯示在更新程式報告檔中。

更新程式會在下列間隔自動執行：2 小時.您可以透過組態編輯或停用自動更新 (組態::更新)。

您可以在控制中心的排程管理員底下建立其他更新工作，讓更新程式在指定的時間間隔內執行這些工作。您也可以選擇手動啓動更新：

– 在控制中心：在 [更新] 功能表與 [狀態] 區段中
– 經由系統匣圖示的內容功能表

您可以經由網際網路從製造商的網路伺服器取得更新。現有的網路連線是 Avira GmbH 下載伺服器的預設連線。您可以在 [組態] 的一般 ::更新底下，變更此預設設定。

8 Avira FireWall ::概觀

Avira FireWall 會監視並規管傳入與傳出電腦系統的資料流量，保護您免於各式各樣的網際網路攻擊與威脅：將依據資訊安全準則，決定是否允許或拒絕傳入或傳出的資料流量或是聆聽連接埠。一旦 Avira FireWall 拒絕了網路活動並封鎖網路連線，您就會收到桌面通知。下列爲設定 Avira FireWall 時可用的選項：

– 在控制中心設定安全性等級

您可以在控制中心定義安全性等級。*低*、*中*和*高*安全性等級各自包含依據封包篩選器所制訂的多項逐層增加的安全性規則。這些安全性規則全都會以預先定義的介面卡規則形式儲存在 [組態] 的 FireWall::介面卡規則底下。

– 在 [網路事件] 視窗中儲存動作

當應用程式第一次嘗試建立網路或是網際網路連線時，會顯示 *[網路事件]* 快顯視窗。*[網路事件]* 視窗可讓使用者選擇是否允許或拒絕應用程式的網路活動。**[儲存此應用程式的動作]** 選項一經啓用，會將動作建立爲應用程式規則，並儲存在組態的 [FireWall::應用程式規則] 底下。將動作儲存在 [網路事件] 視窗中，可針對應用程式的網路活動提供您一組規則。

注意
至於來自信任的供應商的應用程式，系統預設會允許網路存取 (除非介面卡規則禁止網路存取)。您可以選擇從信任的供應商清單中移除供應商。

– 在組態中建立介面卡和應用程式規則

您可以在 [組態] 中，更動預先定義的介面卡規則或是建立新的介面卡規則。當您新增或變更介面卡規則時，FireWall 的安全性等級會自動設爲 *[使用者]* 值。
應用程式規則可讓您定義針對應用程式指定的監視規則：
您可以使用簡單應用程式規則來定義是否要拒絕或允許，以及是否要透過 *[網路事件]* 快顯視窗來處理軟體應用程式的所有網路活動。
您可以在 *[應用程式規則設定]* 的進階組態中，針對應用程式定義不同的封包篩選器，以依據指定的應用程式規則加以執行。

注意
應用程式規則共有兩種不同的模式：*具有權限*與*已篩選*。針對*已篩選*模式下的應用程式規則，會優先處理相關的介面卡規則，亦即會在應用程式規則之後立即執行相關的介面卡規則。因此，系統有可能因爲高安全性等級或對應的介面卡規則而拒絕網路存取。至於在*具有權限*模式下的應用程式規則，則會略過介面卡規則。如果在*具有權限*模式下允許應用程式，一律授予應用程式網路存取功能。

9 備份

建立資料備份時，您可以使用以下各種選項：

透過備份工具備份

您可以使用備份工具來選取或建立備份設定檔，並針對選取的設定檔手動啟動備份作業。

透過排程管理員中的備份工作來備份

[排程管理員] 可讓您選擇建立排程或事件控制的備份工作。[排程管理員] 會自動執行備份工作。如果您想要針對特定資料定期進行備份，這個處理序會特別有用。

10 常見問題集、提示

本章包含有關使用 AntiVir 程式時的疑難排解與其他秘訣的重要資訊。

請參閱下列章節：疑難排解

請參閱下列章節：鍵盤命令

請參閱下列章節：Windows 資訊安全中心

10.1 發生問題時的說明

您可在此找到原因相關資訊與各種疑難雜症的解決方案。

– 出現「*授權檔案無法開啓*」的錯誤訊息。
– AntiVir MailGuard 無法運作。
– 當主機電腦安裝有 Avira FireWall，並將 Avira FireWall 的安全性等級設爲中或高時，虛擬機器 (例如，VMWare、Virtual PC 等) 沒有可用的網路連線。
– 當 Avira FireWall 的安全性等級設爲中或高時，會封鎖虛擬私人網路 (VPN) 連線。
– 透過 TSL 連線傳送的電子郵件已經遭 MailGuard 封鎖。
– 網路聊天無法運作：聊天訊息無法顯示

出現「*授權檔案無法開啓*」的錯誤訊息。

原因：檔案已加密。

▶ 若要啓用授權，您不需要開啓授權檔案，只要將其儲存在程式目錄即可。

嘗試啓動更新時，出現「*下載檔案時連線中斷*」的錯誤訊息。

原因：您的網際網路連線沒有作用。無法順利建立可連接至網際網路 Web 伺服器的連線。

▶ 測試 WWW 或電子郵件之類的其他網際網路服務是否能夠正常運作。如果不行的話，請重新建立網際網路連線。

原因：無法連線 Proxy 伺服器。

▶ 檢查 Proxy 伺服器的登入資料是否已經變更，必要時依據自己的組態加以調整。

原因：您的個人防火牆並未完全核准 update.exe 檔案。

▶ 請確保您的個人防火牆已完全核准 update.exe 檔案。

或是：

▶ 檢查位在一般::更新底下 [組態] (專家模式) 中的您的設定。

無法移動或刪除病毒與惡意程式碼。

原因：檔案已由 Windows 載入，且為作用中。

▶ 更新您的 AntiVir 產品。

▶ 如果您使用 Windows XP 作業系統，請停用 [系統還原]。

▶ 將電腦啓動在 [安全模式]。

▶ 啓動 AntiVir 程式與 [組態] (專家模式)。

▶ 選取 [掃描程式::掃描::檔案::所有檔案]，並於視窗中選取 **[確定]** 以確認。

▶ 針對所有本機磁碟機啓動掃描。

▶ 將電腦啓動在 [一般模式]。

▶ 在一般模式下執行掃描。

▶ 如果沒有找到任何病毒或惡意程式碼，則啓用 [系統還原] (如果可供使用的話)。

系統匣狀態圖示已停用。

原因：AntiVir Guard 已停用。

▶ 在 [AntiVir Guard] 區域底下 [概觀::狀態] 區段中的控制中心，按一下 **[啓用]** 連結。

原因：AntiVir Guard 已遭防火牆封鎖。

▶ 在防火牆的組態中，定義 AntiVir Guard 的一般核准設定。AntiVir Guard 僅能在 127.0.0.1 (localhost) 位址上運作。不會建立網際網路連線。此規則同樣適用於 AntiVir MailGuard。

或是：

▶ 檢查 AntiVir Guard 服務的啓動類型。必要時，請啓用該服務：在工作列中，選取 [開始] | [設定] | [控制台]。按兩下滑鼠來啓動「服務」組態面板 (在 Windows 2000 與 Windows XP 環境下，服務 Applet 位於 [系統管理工具] 子目錄中)。找出項目 *[Avira AntiVir Guard]*。啓動類型必須是「自動」，且狀態必須是「已啓動」。必要時，請選取相關字行並按下 [啓動] 按鈕，手動啓動該服務。出現錯誤訊息時，請檢查事件顯示。

執行資料備份時，電腦變得非常慢。

原因：AntiVir Guard 會在備份程序期間掃描備份程序所使用的所有檔案。

▶ 選取 [組態] (專家模式) 中的 [Guard::掃描::例外]，並輸入備份軟體的處理序名稱。

防火牆在啓動之後，立即回報 AntiVir Guard 和 AntiVir MailGuard。

原因：您可以透過 TCP/IP 網際網路通訊協定，與 AntiVir Guard 和 AntiVir MailGuard 通訊。防火牆可透過此通訊協定監視所有連線。

▶ 在防火牆的組態中，定義 AntiVir Guard 和 AntiVir MailGuard 的一般核准設定。AntiVir Guard 僅能在 127.0.0.1 (localhost) 位址上運作。不會建立網際網路連線。此規則同樣適用於 AntiVir MailGuard。

AntiVir MailGuard 無法運作。

如果 AntiVir MailGuard 發生問題，請藉由下列檢查清單來檢查 AntiVir MailGuard 的功能是否正常運作。

檢查清單

▶ 檢查您的郵件用戶端是否能夠透過 Kerberos、APOP 或 RPA 來登入伺服器。目前不支援這些驗證方法。

▶ 檢查您的郵件用戶端是否能夠透過 SSL (也稱爲 TSL – 傳輸層安全性) 回報伺服器。AntiVir MailGuard 不支援 SSL，因此會終止任何加密 SSL 連線。如果您想要使用不受 MailGuard 保護的加密 SSL 連線，必須對此連線使用不受 MailGuard 監視的連接埠。受到 MailGuard 監視的連接埠可在組態的 MailGuard::掃描底下設定。

▶ AntiVir MailGuard 服務是否爲作用中？必要時，請啓用該服務：在工作列中，選取 [開始] | [設定] | [控制台]。按兩下滑鼠來啓動「服務」組態面板 (在 Windows 2000 與 Windows XP 環境下，服務 Applet 位於 [系統管理工具] 子目錄中)。找出項目 *[Avira AntiVir MailGuard]*。啓動類型必須是「自動」，且狀態必須是「已啓動」。必要時，請選取相關字行並按下 [啓動] 按鈕，手動啓動該服務。出現錯誤訊息時，請檢查事件顯示。如果沒有成功，您可能需要經由 [開始] | [設定] | [控制台] | [新增或移除程式] 來完整解除安裝 " 並重新啓動電腦，接著重新安裝 AntiVir 程式。

一般

▶ 目前無法保護以 SSL (安全通訊端層，通常亦稱爲 TLS (傳輸層安全性)) 加密的 POP3 連線，因此會加以略過。

▶ 目前僅支援透過「密碼」對郵件伺服器進行驗證，目前不支援 "Kerberos" 與 "RPA"。

▶ AntiVir 程式不會檢查外寄電子郵件中的病毒與有害程式。

注意
建議您定期安裝 Microsoft 更新來修補任何安全漏洞。

當主機電腦安裝有 Avira FireWall，並將 Avira FireWall 的安全性等級設爲中或高時，虛擬機器 (例如，VMWare、Virtual PC 等) 沒有可用的網路連線。

如果在執行虛擬機器 (例如 VMWare、Virtual PC 等) 的電腦上安裝 Avira FireWall，當 Avira FireWall 的安全性等級設爲中或高時，防火牆會封鎖虛擬機器的所有網路連線。當安全性等級設爲低時，FireWall 如預期運作。

原因：虛擬機器會透過軟體模擬網路卡運作。此模擬機制會將虛擬系統的資料封包封裝在特殊封包 (UDP 封包) 並透過外部閘道將這些封包引導至原本的主機系統。Avira FireWall 會從安全性等級中開始，拒絕來自外部的封包。

若要避免此行爲發生，請執行下列步驟：

▶ 移至 [控制中心] 並選取 **[線上保護::FireWall]** 區段。

▶ 按一下 **[組態]** 連結。

▶ *[組態]* 對話方塊隨即顯示。您目前位於 *[應用程式規則]* 的組態區段中。

▶ 啓用 **[專家模式]** 選項。

▶ 選取 **[介面卡規則]** 組態區段。

▶ 按一下 **[新增規則]**。

- 選取 *[傳入規則]* 區段中的 **[UDP]**。
- 在規則的 [區段名稱] 中輸入規則**名稱**。
- 按一下 **[確定]**。
- 檢查該規則是否直接優先於 **[拒絕所有 IP 封包]** 規則。

警告
此規則有可能造成危險，因爲它能讓 UDP 封包直接進入而不經過篩選！使用過虛擬機器後，請變更爲原本的安全性等級。

當 Avira FireWall 的安全性等級設爲中或高時，會封鎖虛擬私人網路 (VPN) 連線。

原因：這是因爲最後一個規則 **[拒絕所有 IP 封包]** 會捨棄所有不符合優先性高於該規則之任何一個規則的所有封包。VPN 軟體所發送的封包類型 (所謂的 GRE 封包) 不符合其他類別，因此會遭到此規則篩選。

請使用兩個可拒絕 TCP 和 UDP 封包的新規則來取代 **[拒絕所有 IP 封包]** 規則。如此一來，您就可以允許其他通訊協定的封包進入。

透過 TSL 連線傳送的電子郵件已經遭 MailGuard 封鎖。

原因：MailGuard 目前不支援傳輸層安全性 (TLS：網際網路上的資料傳輸加密通訊協定)。以下爲傳送電子郵件時可用的選項：

- 使用連接埠 25 (SMTP 使用的連接埠) 以外的其他連接埠。這樣會略過 MailGuard 的監視。
- 關閉 TSL 加密連線並停用電子郵件用戶端中的 TSL 支援。
- 在組態的 MailGuard::掃描底下，(暫時) 停用 MailGuard 對外寄電子郵件的監視。

網路聊天無法運作：聊天訊息無法顯示；資料正在載入瀏覽器。

此現象可能會在以 HTTP 通訊協定爲基礎，且內含 'transfer-encoding= chunked' 的聊天中出現。

原因：WebGuard 首先會完整檢查傳送的資料中是否有病毒與有害程式，然後再將資料載入網路瀏覽器。在使用 'transfer-encoding= chunked' 進行資料傳輸期間，WebGuard 無法判斷訊息長度或資料量。

- 請將網路聊天 URL 組態輸入爲例外 (請參閱組態中的 WebGuard::例外)。

10.2 快捷鍵

鍵盤命令 (亦稱爲快捷鍵) 可讓您快速瀏覽與擷取個別模組，並透過程式啓動相關動作。

以下簡介您可用的鍵盤命令。請在對應的說明章節中，找到各項功能的相關介紹。

10.2.1 在對話方塊中

快捷鍵	**Description**
Ctrl + Tab Ctrl + Page down	控制中心的瀏覽 移至下一節。
Ctrl + Shift + Tab Ctrl + Page up	控制中心的瀏覽 移至上一節。
←↑→↓	組態區段的瀏覽 首先，使用滑鼠將焦點放在組態區段。
Tab	變更至下一個選項或選項群組。
Shift + Tab	變更至上一個選項或選項群組。
←↑→↓	在標示的下拉式清單中，或於選項群組中的各個選項之間切換選項。
空格鍵	啓用或停用核取方塊 (作用中的選項必須是核取方塊)。
Alt + 含底線的字母	選取選項或啓動命令。
Alt + ↓ F4	開啓選取的下拉式清單。
Esc	關閉選取的下拉式清單。 取消命令與關閉對話方塊。
Enter	針對作用中的選項或按鈕啓動命令。

10.2.2 在說明中

快捷鍵	**Description**
Alt + 空格鍵	顯示系統功能表。
Alt + Tab	切換說明與其他開啓的視窗。
Alt + F4	關閉說明。
Shift + F10	顯示說明的內容功能表。
Ctrl + Tab	移至瀏覽視窗的下一個區段。
Ctrl + Shift + Tab	移至瀏覽視窗的上一個區段。
Page up	變更至顯示在內容、索引或是搜尋結果清單上方的主題。
Page down	變更至顯示在內容、索引或是搜尋結果清單下方的主題。
Page up	瀏覽主題。

Page down	

10.2.3 在控制中心中

一般

快捷鍵	Description
F1	顯示說明
Alt + F4	關閉控制中心
F5	重新整理
F8	開啓組態
F9	開始更新

掃描區段

快捷鍵	Description
F2	重新命名選取的設定檔
F3	以選取的設定檔開始掃描
F4	爲選取的設定檔建立桌面連結
Ins	建立新的設定檔
Del	刪除選取的設定檔

FireWall 區段

快捷鍵	Description
Return	屬性

隔離區區段

快捷鍵	Description
F2	重新掃描物件
F3	還原物件
F4	傳送物件
F6	將物件還原至...
Return	屬性
Ins	新增檔案
Del	刪除物件

排程管理員區段

快捷鍵	Description
F2	編輯工作
Return	屬性
Ins	插入新工作
Del	刪除工作

報告區段

快捷鍵	Description
F3	顯示報告檔
F4	列印報告檔
Return	顯示報告
Del	刪除報告

事件區段

快捷鍵	Description
F3	匯出事件
Return	顯示事件
Del	刪除事件

10.3 Windows 資訊安全中心

- Windows XP Service Pack 2 或更新版本 -

10.3.1 一般

Windows 資訊安全中心會檢查電腦狀態以了解重要的安全層面。

一旦在這些要點中偵測到問題 (例如，過時的防毒程式)，資訊安全中心就會發出警示並針對如何保護電腦安全提供相關建議。

10.3.2 Windows 資訊安全中心和您的 AntiVir 程式

FireWall

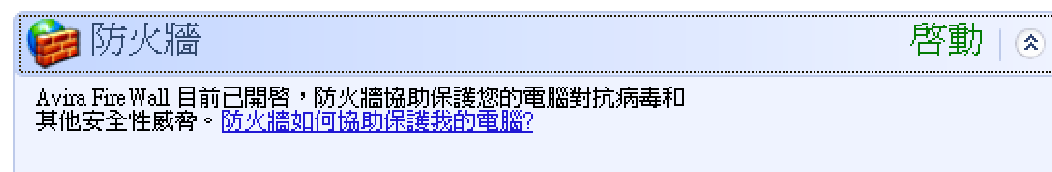
您可能會從資訊安全中心收到有關防火牆的下列資訊：

– FireWall 啓用/FireWall 啓動

– FireWall 停用/FireWall 關閉

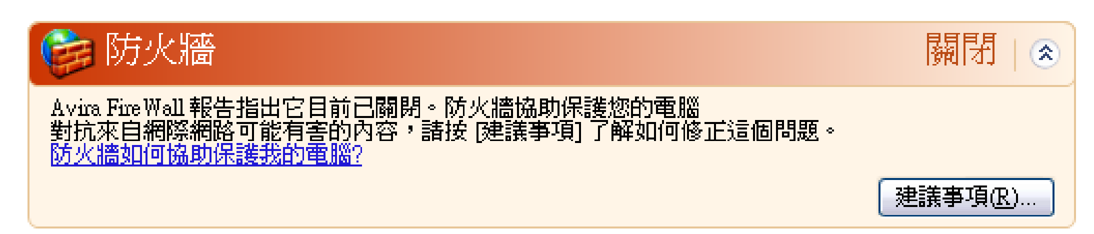
FireWall 啓用/FireWall 關閉

完成安裝 AntiVir 程式且關閉 Windows 防火牆之後，您將收到下列訊息：



FireWall 停用/FireWall 關閉

當您停用 Avira FireWall 時，將會立即收到下列訊息：



注意
您可以經由 控制中心的 [狀態] 索引標籤，啓用或停用 Avira FireWall。

警告
如果您將 Avira FireWall 關閉，電腦便無法繼續防堵未授權的使用者透過網路或網際網路擅自存取。

防毒軟體/抵禦惡意軟體

您可能會從 Windows 資訊安全中心收到有關防毒的下列資訊：

找不到防毒保護

防毒保護已非最新狀態

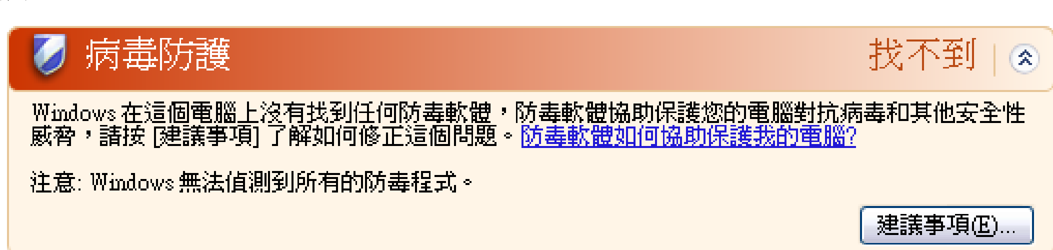
防毒保護已開啓

防毒保護已關閉

防毒保護未受監視

找不到防毒保護

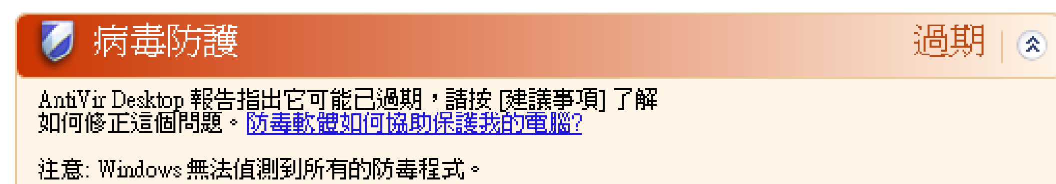
當 Windows 資訊安全中心無法在您的電腦上找到任何防毒軟體時，就會顯示此類資訊。



注意
請在電腦上安裝您的 AntiVir 程式，協助電腦防禦病毒與其他有害程式！

防毒保護已非最新狀態

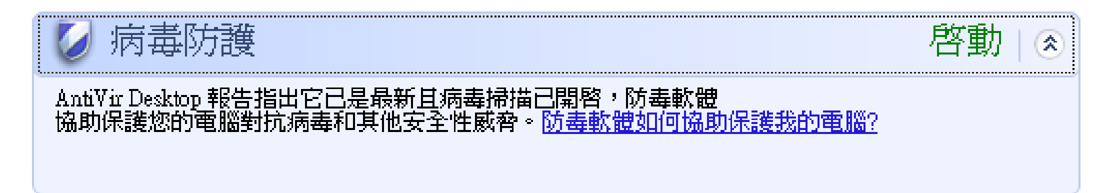
如果您先安裝 Windows XP Service Pack 2 或 Windows Vista 後再安裝您的 AntiVir 程式，或是將 Windows XP Service Pack 2 或 Windows Vista 安裝在已經安裝了 AntiVir 程式的系統上，會收到下列訊息：



注意
爲了讓 Windows 資訊安全中心將 AntiVir 程式識別爲最新狀態，請在安裝後執行更新。請執行更新來更新系統。

防毒保護已開啓

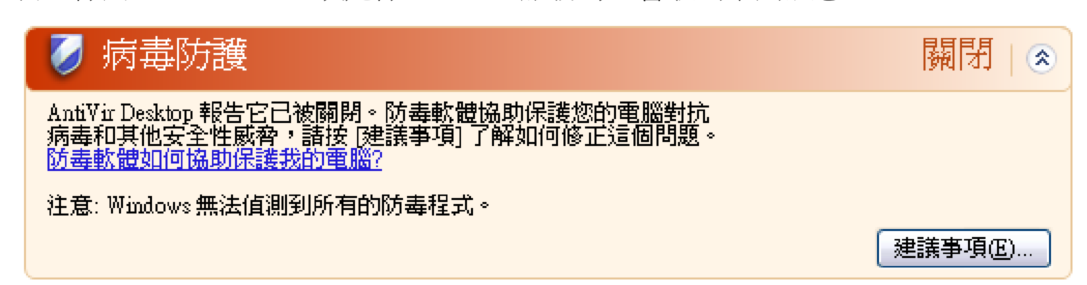
在安裝了 AntiVir 程式與後續更新之後，您將會收到下列訊息：



您的 AntiVir 程式現在已是最新的，並已啓用 AntiVir Guard。

防毒保護已關閉

當您停用 AntiVir Guard 或是停止 Guard 服務時，會收到下列訊息。

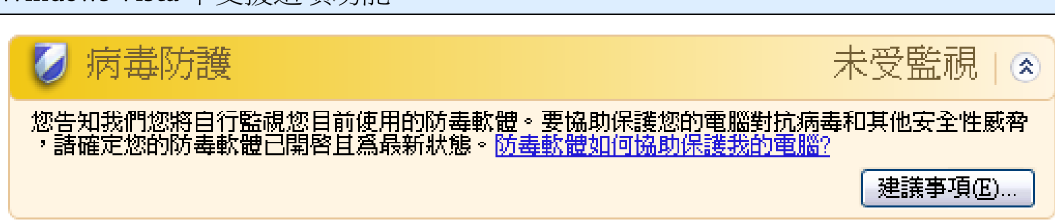


注意
您可以從控制中心的 [概觀::狀態] 區段中，啓用或停用 AntiVir Guard。您也可以藉由工作列中的小紅傘圖示是否開啓，來判斷 AntiVir Guard 是否已經啓用。

防毒保護未受監視

如果您從 Windows 資訊安全中心收到下列訊息，表示您已決定自行監視防毒軟體的狀態。

注意
Windows Vista 不支援這項功能。



注意
您的 AntiVir 程式支援 Windows 資訊安全中心。您隨時可以透過 [建議] 按鈕來啓用這個選項。

注意
即使您已經安裝 Windows XP Service Pack 2 或 Windows Vista，仍舊需要防毒解決方案。雖然 Windows XP Service Pack 2 會監視您的防毒軟體，本身卻不含任何防毒功能。因此，如果沒有配備其他防毒解決方案，您將無法防範各種病毒與其他惡意程式碼！

11 病毒與其他資訊

11.1 延伸的威脅類別

撥號木馬程式 (DIALER)

網際網路上有某些服務必須付費。在德國，這類服務都是透過 0190/0900 開頭號碼的撥號木馬程式來開立發票 (在奧地利與瑞士則是透過 09x0 開頭的號碼；在德國，這組號碼會在轉接途中變更為 09x0 開頭)。一旦安裝在電腦上，這些木馬程式可保證以合適的優惠費率號碼來連線，且各地收費方式都不同。

透過電話帳單來行銷線上內容是合法的，而且對使用者有利。真正的撥號木馬程式毫無疑問地可由使用者應用在特定用途上。這些木馬程式只能在使用者同意 (經由完整、不模糊而且可清楚辨識的標籤或要求) 下安裝在使用者的電腦上。真正的撥號木馬程式會清楚顯示撥接程序。此外，真正的撥號木馬程式會明確無誤地告知產生的費用。

不過，有些撥號木馬程式會透過模擬兩可的方式，甚至以欺騙的手法偷偷地安裝在電腦上。例如，它們會取代 ISP (網際網路服務供應商) 的網際網路使用者預設資料通訊連結，並在每次成功連線後，撥出 0190/0900 開頭的號碼 (會產生費用而且經常貴得嚇人)。受影響的使用者大概在下一次帳單抵達之前，都不會注意到電腦上有害的 0190/0900 撥號木馬程式已經在每次連線時撥出優惠費率號碼，導致電話帳單費用暴增。

建議您直接要求電話業者封鎖這類號碼範圍以便立即防範不需要的撥號木馬程式 (0190/0900 撥號木馬程式)。

您的 AntiVir 程式預設會偵測到熟悉的撥號木馬程式。

[撥號木馬程式] 選項一經啓用 (於組態中延伸的威脅類別底下勾選)，您會在偵測到撥號木馬程式時收到對應的警示。現在您可以直接刪除可能有害的 0190/0900 撥號木馬程式。不過，如果是想要的撥接程式，您可以將其宣告為例外檔案，日後便不會加以掃描。

遊戲 (GAMES)

到處都有網咖可供玩遊戲，不過工作場所不見得有 (除非在午休時間)。不過，隨著網際網路上的可下載遊戲越來越多，公司員工與公僕們也開始迷上踩地雷之類的小遊戲。您可以經由網際網路下載一系列遊戲。電子郵件遊戲也開始越來越盛行：為數眾多的變種遊戲開始流通，從簡單的西洋棋到艦隊遊戲等 (包括水雷對戰) 不一而足：夥伴則是經由電子郵件程式來回應合作夥伴對應的行動。

各項研究顯示投入到電腦遊戲的工作時數已經達到相當的經濟規模。因此，不難想像越來越多公司開始考慮禁止員工利用公司電腦來玩電腦遊戲。

您的 AntiVir 程式會辨識電腦遊戲。**[遊戲]** 選項一經啓用 (於組態中威脅類別底下勾選)，您會在 AntiVir 程式偵測到遊戲時收到對應的警示。講真的，遊戲現在已經沒有發展空間，因為您可以直接加以刪除。

惡作劇程式 (JOKES)

惡作劇程式單純地只是想要嚇嚇某人，或是博君一笑，沒有任何惡意。惡作劇程式一經載入，電腦通常會在某個運作時間點播放一段音樂或是在螢幕上顯示一些奇怪的畫面。諸如磁碟機中的洗衣機 (DRAIN.COM) 或是會吃掉畫面的怪物 (BUGSRES.COM) 等，都是惡作劇程式的例子。

但是，請注意！所有的惡作劇程式徵狀有可能同時源自於病毒或特洛伊木馬程式。使用者至少會受到極大的驚嚇，或是過度恐慌，以致於造成真正的傷害。

多虧了掃描與識別常式延伸功能，AntiVir 程式可以偵測到惡作劇程式並在必要時將這些程式當成有害的程式予以消除。**[惡作劇程式]** 選項一經啓用 (於組態中威脅類別底下勾選)，您會在偵測到惡作劇程式時收到對應的警示。

安全性隱私風險 (SPR)

當軟體會破壞系統安全、初始有害的程式活動、損害您的隱私或是窺視您的使用者行爲時，可能已經成爲有害的程式。

您的 AntiVir 程式可偵測「安全性隱私風險 (SPR)」軟體。**[安全性隱私風險]** (SPR) 選項一經啓用 (於組態中延伸的威脅類別底下勾選)，您會在 AntiVir 程式偵測到此類軟體時收到對應的警示。

後門程式用戶端 (BDC)

後門伺服器程式是基於竊取資料或操縱電腦的目的，在使用者不知情的狀況下私自混進系統中。這種程式可以由第三方利用後門控制軟體 (用戶端) 透過網際網路或內部網路進行控制。

您的 AntiVir 程式可辨識「後門控制軟體」。**[後門控制軟體]** (BDC) 選項一經啓用 (於組態中延伸的威脅類別底下勾選)，您會在 AntiVir 程式偵測到此類軟體時收到對應的警示。

廣告軟體/間諜軟體 (ADSPY)

這些可能是有害的軟體，因爲它們會顯示廣告，或是在使用者不知情或未經使用者同意的情況下，將使用者個人資料傳送給第三方。

您的 AntiVir 程式可辨識「廣告軟體/間諜軟體」。**[廣告軟體/間諜軟體]** (ADSPY) 選項一經啓用 (於組態中延伸的威脅類別底下勾選)，您會在 AntiVir 程式偵測到廣告軟體或間諜軟體時收到對應的警示。

少見的執行階段壓縮程式 (PCK)

使用少見的執行階段壓縮程式來壓縮並因此而歸類爲可疑檔案的檔案。

您的 AntiVir 程式可辨識「少見的執行階段壓縮程式 (PCK)」。**[少見的執行階段壓縮程式]** (PCK) 選項一經啓用 (於組態中延伸的威脅類別底下勾選)，您會在 AntiVir 程式偵測到此類壓縮程式時收到對應的警示。

雙重副檔名檔案 (HEUR-DBLEXT)

以可疑的方式來隱藏真實副檔名的可執行檔。這種僞裝的方法是惡意程式碼慣用的伎倆。

您的 AntiVir 程式可辨識「雙重副檔名檔案 (HEUR-DBLEXT)」。**[雙重副檔名檔案]** (HEUR-DBLEXT) 選項一經啓用 (於組態中延伸的威脅類別底下勾選)，您會在 AntiVir 程式偵測到此類檔案時收到對應的警示。

網路釣魚

網路釣魚 (又稱爲*品牌詐騙*) 是一種聰明的資料竊盜手法，主要瞄準網際網路服務供應商、銀行、網路銀行服務、註冊機關之類團體的客戶或潛在客戶下手。
當您在網際網路上提交電子郵件地址、填寫線上表單存取新聞群組或網站時，「網路蜘蛛」就會趁機竊取您的資料，並在尚未得到您的允許情況下，私自用來進行詐騙或其他犯罪行爲。

您的 AntiVir 程式可辨識「網路釣魚」。**[網路釣魚]** (SPR) 選項一經啓用 (於組態中延伸的威脅類別底下勾選)，您會在 AntiVir 程式偵測到此類行爲時收到對應的警示。

應用程式 (APPL)

APPL 一詞表示使用的應用程式可能有風險，或其來源很可疑。

您的 AntiVir 程式可辨識「應用程式 (APPL)」。**[應用程式]** (APPL) 選項一經啓用 (於組態中延伸的威脅類別底下勾選)，您會在 AntiVir 程式偵測到此類行爲時收到對應的警示。

11.2 病毒與其他惡意程式碼

廣告軟體

廣告軟體指的是透過電腦畫面上顯示的訊息列來呈現橫幅廣告或快顯視窗的軟體。這些廣告通常無法移除且會持續顯示。在資料安全方面，連線資料可以讓人從中得出許多使用行爲上的資訊，因此也會造成一些問題。

後門程式

後門程式會藉由繞過電腦存取安全機制來取得電腦的存取權。

在背景執行的某個程式會開啓方便之門，賦予攻擊者無限的權限。使用者的個人資料可能會遭後門程式竊取。而且主要是被用來在相關系統上植入更多的電腦病毒和蠕蟲。

開機病毒

硬碟的開機或主要開機磁區主要會受到開機磁區病毒感染。這些病毒會覆寫系統執行時所需的重要資訊。出現的怪異行爲之一爲：電腦系統從此無法載入...

傀儡網路

定義爲遠端 (網際網路上) 電腦網路的傀儡網路，包含許多可互相通訊的傀儡電腦。殭屍網路由一系列遭到破解的機器組成，這些機器會在一般命令與控制基礎結構下執行一些程式 (通常稱爲蠕蟲與特洛伊木馬程式)。傀儡網路有多重目的，包括阻斷服務攻擊等等，通常會在電腦使用者不知情的情況下執行。傀儡網路最可怕的地方在於其規模可達到成千上萬台電腦，流量總和甚至會超過最常設的網際網路頻寬限制。

惡意探索程式碼

惡意探索程式碼 (安全漏洞) 是一種電腦程式或指令碼，它會利用錯誤、異常或漏洞來提升權限或是讓電腦系統觸發阻斷服務。例如，有一種惡意探索程式碼會透過受操控的資料套件從網際網路發動攻擊。這些程式碼會滲透到程式當中以取得更高的存取權。

謊報惡意程式

網際網路與其他網路使用者多年來紛紛收到刻意透過電子郵件散播的病毒警示。這些警示會透過電子郵件散播出去，並要求收件者盡可能將它們傳送給最多的同事與其他使用者以便讓每個人都知道危險。

誘捕機制

誘捕機制是安裝在網路上的一種服務 (程式或伺服器)。它的功能在於監控網路和記錄攻擊事件。合法的使用者不會知道這項服務，正因爲如此，也就沒人去注意到相關問題。如果攻擊者探查網路上的弱點並利用誘捕機制所提供的服務，就會加以記錄並觸發警示。

巨集病毒

巨集病毒指的是以應用程式巨集語言所撰寫的小型程式 (例如，WinWord 6.0 底下運作的 WordBasic)，通常只能透過這類應用程式文件來散播。因爲這個原因，人們也將之稱爲文件病毒。這類病毒若要發揮作用，對應的應用程式必須啓動，而且任何一項已感染病毒的巨集也必須執行才行。與「一般」病毒不同的是，巨集病毒不會因此攻擊可執行檔，而是攻擊對應主機應用程式的文件。

網址嫁接

網址嫁接技術會操控網頁瀏覽器的主機檔案，將查詢轉向假冒的網站。這是傳統網路釣魚的翻新手法。網址嫁接詐騙份子將假冒的網站儲存在自己管理的大量伺服器陣列中。各種 DNS 攻擊類型都可歸類到網址嫁接。在主機檔案遭到操控的情況下，攻擊者可透過特洛伊木馬程式或是病毒對某個系統進行特別操控。影響所及，系統現在只能存取假冒的網站，就算輸入了正確的網址也沒用。

網路釣魚

網路釣魚指的是瞄準網際網路使用者的個人資料下手的詐騙手法。網路釣客通常會將看似正式的信函寄送給被害人，並透過這類郵件引誘被害人在不疑有他的情況下揭露機密資訊，尤其是使用者名稱與密碼或是網路銀行帳戶的 PIN 碼或 TAN 碼。透過竊取的存取資料，網路釣客可以假冒被害人的身分來執行一連串的交易行為。可確定的一點是，銀行與保險公司絕對不會透過電子郵件、簡訊或是電話要求提供信用卡號碼、PIN 碼、TAN 碼或是其他存取資料。

千面人病毒

千面人病毒真的是千變萬化。它們會更改自身的程式碼，因此偵測起來非常困難。

程式病毒

所謂的電腦病毒，指的是在執行之後能夠將自身附加到其他程式上，並引發感染。與邏輯炸彈和特洛伊木馬程式不同的是，這些病毒會自我分裂繁殖。這種病毒必須搭配宿主程式以便植入有毒的程式碼，這點與蠕蟲不同。通常宿主程式的執行狀況並不會改變。

Rootkit

Rootkit 是一群軟體工具，會在成功滲透電腦系統之後進行安裝並隱藏滲透者的登入資料、隱藏相關處理序與記錄資料。一般而言，就是讓自己隱形起來。它們會嘗試更新已經安裝的間諜軟體，並重新安裝已刪除的間諜軟體。

指令碼病毒與蠕蟲

這類病毒的程式非常容易編寫，而且只要具備所需的技術，在幾小時內就能透過電子郵件散播到全世界。

指令碼病毒與蠕蟲會使用 Javascript、VBScript 之類的指令碼語言滲透到其他新的指令碼中，或呼叫作業系統功能來進行散播。這種情況通常會藉由電子郵件或是在交換檔案 (或文件) 期間發生。

蠕蟲是一種會自我分裂繁殖的程式，但不會感染宿主。因此，蠕蟲並不會成為其他程式序列的一部分。蠕蟲通常只會經由安全措施有限的系統，滲透到任何受損的程式中。

間諜軟體

間諜軟體指的是會在使用者不知情的情況下，攔截或掌控部分電腦作業內容的間諜程式。間諜軟體是專為攻擊受感染的電腦以獲取商業利益而設計。

特洛伊木馬程式 (簡稱特洛伊木馬)

特洛伊木馬程式目前很常見。特洛伊木馬程式包括會假裝具有特殊功能，但是在執行之後便顯露出真面目，而且在大多數情況下會執行具有毀滅性的功能。特洛伊木馬程式無法自我分裂繁殖，這點與其他病毒和蠕蟲不同。這類程式大部分都有一個有趣的名稱 (SEX.EXE 或 STARTME.EXE)，用意就是引起使用者注意，進而啓動特洛伊木馬程式。這類程式一經執行，馬上會開始活躍，並可能開始大肆破壞，例如將硬碟格式化。病毒植入程式是特洛伊木馬程式的特殊型態，可以將病毒嵌入電腦系統當中。

僵屍電腦

僵屍電腦是受到惡意程式攻擊的電腦，可讓駭客透過遠端控制來爲所欲爲，藉此達到其犯罪目的。例如，受感染的電腦會發動阻斷服務 (DoS) 攻擊，或是散播垃圾郵件與網路釣魚郵件。

12 資訊與服務

本章包含我們的連絡資訊。

請參閱下列章節：連絡地址

請參閱下列章節：技術支援

請參閱下列章節：可疑的檔案

請參閱下列章節：回報誤判

請參閱下列章節：歡迎您提供安全性提升意見

12.1 連絡地址

如果您對於 AntiVir 產品系列還有任何疑問或要求的話，我們將很樂意提供協助。請從控制中心的說明::關於 Avira Premium Security Suite 底下找到我們的連絡地址。

12.2 技術支援

Avira 支援可提供您可靠的協助，幫您解答各式各樣的問題或是解決技術問題。

您可以從我們的網站 ，找到我們全方位支援服務的所有必要資訊：

http://www.avira.tw/premium-suite-support

以便我們快速處理並提供您值得信賴的協助。請您備妥下列資訊：

- **授權資訊**。您可以從下列功能表項目找出程式介面：說明 ::關於 Avira Premium Security Suite ::授權資訊
- **版本資訊**。您可以從下列功能表項目找出程式介面：說明 ::關於 Avira Premium Security Suite::版本資訊功能表項目底下，可找到這項資訊。
- **作業系統版本**與任何一項安裝的 Service Pack。
- **安裝的軟體套件**，例如，其他廠商的防毒軟體。
- 程式或報告檔案的**準確訊息**。

12.3 可疑的檔案

請將我們的產品無法偵測或是移除的病毒，或是可疑的檔案寄給我們。您可以透過下列方式進行。

- 在隔離區管理員 (位於 控制中心) 中，識別檔案，並使用內容功能表或對應的按鈕來選取傳送檔案項目。

– 將所需的檔案壓縮成 WinZIP、PKZip、Arj 之類的格式，並以電子郵件附件方式寄至下列地址：
  virus-premium-suite@avira.tw
  由於某些電子郵件閘道會配置防毒軟體，請同時提供加密壓縮的檔案 (記得告訴我們解壓縮密碼)。

您也可以透過我們的網站，將可疑的檔案傳送給我們：http://www.avira.tw/sample-upload

12.4 回報誤判

如果您認爲 AntiVir 程式回報的檔案極有可能是「沒問題」，請將所需的檔案壓縮起來 (WinZIP、PKZip、Arj 等格式) 並以電子郵件附件方式寄至下列地址：

– virus-premium-suite@avira.tw

由於某些電子郵件閘道會配置防毒軟體，請同時提供加密壓縮的檔案 (記得告訴我們解壓縮密碼)。

12.5 您的意見將協助我們提供更完善的資訊安全服務

在 Avira，我們最重視客戶的安全保障。'因此，在每一項產品發佈之前，我們不只藉由內部專家團隊來測試每一項 Avira GmbH 解決方案的品質與安全性，同時相當重視資訊安全相關漏洞，並花費同樣的精力與成本來用心處置。

如果您在我們的產品中發現任何安全漏洞，請以電子郵件將相關意見寄至下列地址：

vulnerabilities-premium-suite@avira.tw

13 參照：組態選項

組態參照會記錄所有的可用組態選項。

13.1 掃描程式

[組態] 的 [掃描程式] 區段負責指定掃描的組態。

13.1.1 掃描

在此您可針對指定掃描定義掃描常式的基本行爲。如果您選取了要以指定掃描來掃描的特定目錄，依據組態而定，掃描程式的掃描行爲可能會是：

– 帶有特定掃描威力 (優先順序)、
– 同時掃描開機磁區與主記憶體、
– 掃描特定或所有的開機磁區與主記憶體、
– 掃描目錄中的所有檔案或選取的檔案。

檔案

掃描程式可以透過篩選器來專門掃描帶有特定副檔名 (類型) 的檔案。

所有檔案

此選項一經啓用，所有檔案 (不論其內容或副檔名爲何) 都會進行病毒或惡意程式的掃描。不使用任何篩選器。

注意
一旦啓用所有檔案選項，便無法選取**副檔名**按鈕。

智慧副檔名辨識

此選項一經啓用，此程式會自動選擇要掃描病毒或有害程式的檔案。這表示您的 AntiVir 程式會依據檔案內容決定是否要加以掃描。此程序在速度上會比透過使用副檔名清單方式來得緩慢，不過卻比較安全，因爲並不只有針對特定副檔名才進行掃描。系統不只預設啓用此選項，也建議使用這個選項。

注意
智慧副檔名辨識選項一經啓用，便無法選取**副檔名**按鈕。

使用副檔名清單

此選項一經啓用，只會掃描帶有指定副檔名的檔案。所有可能包含病毒與有害程式的檔案類型都會預先設定好。此清單可經由 "**[副檔名]**" 按鈕手動加以編輯。

注意
此選項一經啓用，而且您已從清單中刪除所有特定副檔名項目時，會在**副檔名**按鈕底下顯示 [無副檔名] 字樣。""

副檔名

藉由此按鈕，會開啓一個對話方塊並顯示所有於 "**[使用副檔名清單]**" 模式中掃描的所有副檔名。系統會針對副檔名設定預設項目，不過您可以新增或刪除這些項目。

注意
請注意，預設清單會依版本不同而有所差異。

其他設定

掃描所選取磁碟機的開機磁區(&B)

此選項一經啓用，掃描程式會針對選取的指定掃描磁碟機掃描其中的開機磁區。此選項會啓用爲預設值。

掃描主開機磁區

此選項一經啓用，掃描程式會針對系統中使用的硬碟掃描其中的主開機磁區。

略過離線檔案

此選項一經啓用，直接掃描會在掃描期間完全略過所謂的離線檔案。亦即，不會掃描這些檔案當中是否有病毒與有害程式。舉例來說，離線檔案指的是由所謂的階層儲存管理系統 (HSMS) 從硬碟實際移動到磁帶的所有檔案。此選項會啓用爲預設值。

系統檔案完整性檢查

此選項一經啓用，每次進行指定掃描時，系統會針對最重要的 Windows 系統檔案進行特別安全檢查，查看是否有任何檔案遭到惡意程式碼變更。如果偵測到修改的檔案，會將此檔案報告爲可疑。這項功能會使用大量的電腦資源。因此預設會停用此選項。

重要
此選項僅能用於 Windows Vista (含) 以上版本。

注意
如果您是使用可修改系統檔案並依據個人需求調整開機或開始畫面的第三方工具，不應使用此選項。這類工具的範例爲 Skinpacks、TuneUp 公用程式或 Vista Customization。

最佳化掃描

此選項一經啓用，掃描程式的掃描期間會以最高效率來運用處理器資源。爲了不影響效能，最佳化掃描只會記錄爲標準等級。

注意
只能在多處理器系統下使用此選項。如果

追蹤符號連結

此選項一經啓用，掃描程式所執行的掃描會追蹤掃描設定檔或選取目錄中的所有符號連結，並掃描連結檔中是否有病毒與惡意程式碼。Windows 2000 不支援而且會停用此選項。

重要
此選項並未包含任何捷徑，而是專門指檔案系統中清楚易見的符號連結 (由 mklink.exe 產生) 或連接點 (由 junction.exe 產生)。

先搜尋 Rootkit 再掃描

此選項一經啓用，啓動掃描後掃描程式會掃描 Windows 系統目錄中所謂的捷徑是否有作用中的 Rootkit。此處理序不像掃描設定檔 "**[掃描 Rootkit]**" 能夠完整地掃描電腦中是否有作用中的 Rootkit，但是執行效能卻是快上許多。

重要
Rootkit 掃描不適用於 Windows XP 64 位元！

掃描登錄

此選項一經啟用，會掃描登錄中是否有惡意程式碼的參照。

掃描程序

允許停止掃描程式

此選項一經啟用，您隨時可以經由 [Luke Filewalker] 視窗中的 "**[停止]**" 按鈕來終止病毒或有害程式的掃描。""一旦停用此設定，[Luke Filewalker] 視窗中的 **[停止]** 按鈕會呈現灰色背景。""因此，您無法提前終止掃描處理序！此選項會啟用爲預設值。

掃描程式優先順序

透過指定掃描，掃描程式可以區分優先順序等級。只有當工作站上同時執行多個處理序，此設定才有作用。此選項會影響掃描速度。

低

只有當其他處理序都不需要運算時，才會將處理器時間分配給掃描程式，亦即，當作業系統中只執行掃描程式時，將保持全速運作。總之，這時使用其他程式將可獲得最佳效率：當掃描程式持續在背景中運作時，如果其他程式需要運算資源，電腦便可以更快速地回應。系統不只預設啟用此選項，也建議使用這個選項。

中

掃描程式將以正常優先順序來執行。作業系統會針對所有處理序配置等量的處理器資源。在特定情況下，使用其他應用程式的效能可能會受到影響。

高

掃描程式具有最高的優先順序。同時使用其他應用程式幾乎不可能。不過，掃描程式會全速完成掃描。

13.1.1.1. 偵測有所發現時採取的動作

偵測有所發現時採取的動作

您可以定義當偵測到病毒或有害程式時，掃描程式要執行的動作。

互動式

此選項一經啟用，會在對話方塊中顯示掃描程式掃描的結果。使用掃描程式掃描時，在掃描結束時，您會收到一則警示，內含受影響的檔案清單。您可以使用即時線上功能表，針對各種受感染的檔案選取要執行的動作。您可以針對所有受感染的檔案執行標準動作，或是取消掃描程式。

注意
在掃描程式通知中，預設會預先選取 [移至隔離區] 動作。可經由內容功能表選取進一步動作。

如需詳細資訊，按一下此處。

自動

此選項一經啟用，偵測到病毒時將不會出現任何對話方塊。掃描程式會根據您在這個區段中預先定義爲主要和次要動作的設定來反應。

備份至隔離區

此選項一經啓用，掃描程式會在執行要求的主要或次要動作之前建立備份複本。如果檔案具有參考價值，可以將備份複本儲存在隔離區以便稍後還原。您也可以將備份複本傳送給 Avira 惡意程式碼研究中心做進一步調查。

主要動作

主要動作是掃描程式發現病毒或有害程式時優先執行的動作。如果選取了 "**[修復]** " 選項，但卻無法修復受影響的檔案，便會執行在 "**[次要動作]**" 底下選取的動作。

注意
次要動作選項必須當您已選取 **[修復]** 設定 (位於主要動作底下) 時才能選取。

修復

此選項一經啓用，掃描程式會自動修復受影響的檔案。如果掃描程式無法修復受影響的檔案，會執行在次要動作底下選取的動作。

注意
我們建議使用自動修復動作，不過這意味著掃描程式將修改工作站上的檔案。

刪除

此選項一經啓用，會刪除檔案。此處理序在速度上會比 [覆寫並刪除] 要來得快速。

覆寫並刪除

此選項一經啓用，掃描程式會先使用預設模式來覆寫檔案，再加以刪除。此檔案無法還原。

重新命名

此選項一經啓用，掃描程式會重新命名檔案。如此將無法再直接存取這些檔案 (例如按兩下滑鼠)。檔案可以在之後修復並重新賦予其原始名稱。

略過

此選項一經啓用，可允許存取檔案，並保留檔案原貌不動。

警告
工作站上受影響的檔案仍會繼續運作！此做法可能會對工作站造成嚴重的傷害！

隔離區

此選項一經啓用，掃描程式會將檔案移至隔離區。稍後可以修復這些檔案，必要時也可將其傳送至 Avira 惡意程式碼研究中心。

次要動作

"**[次要動作]** "選項必須當您已選取 **[修復]** 設定 (位於 "**[主要動作]**" 底下) 時才能選取。透過這個選項，現在您可以決定要對無法修復的檔案採取哪些處置方式。

刪除

此選項一經啓用，會刪除檔案。此處理序在速度上會比 [覆寫並刪除] 要來得快速。

覆寫並刪除

此選項一經啓用，掃描程式會先使用預設模式來覆寫檔案，再加以刪除 (抹淨)。此檔案無法還原。

重新命名

此選項一經啓用，掃描程式會重新命名檔案。如此將無法再直接存取這些檔案 (例如按兩下滑鼠)。檔案可以在之後修復並重新賦予其原始名稱。

略過

此選項一經啓用，可允許存取檔案，並保留檔案原貌不動。

警告
工作站上受影響的檔案仍會繼續運作！此做法可能會對工作站造成嚴重的傷害！

隔離區

此選項一經啓用，掃描程式會將檔案移至隔離區。稍後可以修復這些檔案，必要時也可將其傳送至 Avira 惡意程式碼研究中心。

注意
若您已選取 **[刪除]** 或 **[覆寫並刪除]** 做爲主要或次要動作，請注意下列事項：當啓發式掃毒模式偵測到病毒時，並不會刪除受影響的檔案，而是將之移至隔離區。

掃描封存時，掃描程式會使用遞迴掃描：封存內的封存在經過解壓縮之後，會掃描其中是否有病毒與有害程式。檔案經過掃描之後，會解壓縮並重新掃描一遍。

掃描封存

此選項一經啓用，會掃描封存清單中選取的封存。此選項會啓用爲預設值。

所有封存類型

此選項一經啓用，會選取封存清單中的所有封存類型並加以掃描。

智慧副檔名辨識

此選項一經啓用，即使副檔名與一般副檔名有所差異，掃描程式還是會偵測檔案是否爲壓縮檔案格式 (封存)，並加以掃描。不過，爲此每個檔案必須開啓，而這點會使掃描速度變慢。例如：如果 *.zip 封存含有 *.xyz 的副檔名，則掃描程式也會解壓縮此封存並加以掃描。此選項會啓用爲預設值。

注意
僅支援封存清單中標示的封存類型。

遞迴深度

解壓縮與掃描遞迴封存需要大量的電腦運算時間與資源。此選項一經啓用，您可以將多重壓縮封存中的掃描深度限制在特定的壓縮層級數量 (最大遞迴深度)。此舉可節省時間與電腦資源。

注意
爲了在封存中找到病毒或有害程式，掃描程式最多必須掃描至病毒或有害程式所在的遞迴層級。

遞迴深度上限

若要輸入最大遞迴深度，必須啓用限制遞迴深度。
您可以直接輸入要求的遞迴深度，或是透過輸入欄位上的向右箭頭按鍵。允許的值介於 1 到 99。建議的標準值爲 20。

預設值

此按鈕會還原用於掃描封存的預先定義值。

封存

您可以在此顯示區域，設定掃描程式應該掃描的封存。爲此，您必須選取相關項目。

13.1.1.2. 例外

要讓掃描程式略過的檔案物件

此視窗中的清單包含當掃描程式掃描病毒或有害程式時，不應包含的檔案與路徑。

在此請盡可能不要輸入例外項目，否則請輸入無論如何一定得排除在正常掃描作業之外的項目。在您將檔案包含在此清單之前，建議您一律加以掃描，確定其中沒有病毒或有害程式。

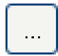
注意
清單中的項目結果總數不得超過 6000 個字元。

警告
這些檔案不會包含在掃描作業中！

注意
此清單上的檔案已全部記錄在報告檔案中。請隨時檢查報告檔案中是否有未掃描的檔案，因爲您先前排除檔案的原因現在可能已經不存在。在此情況下，請再次從此清單中移除檔案名稱。

輸入方塊

您可以在此輸入方塊中輸入不要包含在指定掃描中的檔案物件名稱。預設不會輸入任何檔案物件。



此按鈕會開啓新的視窗，供您選取必要的檔案或路徑。
如果您輸入包含完整路徑的檔案名稱，只有此檔案不會接受掃描。如果您輸入不含路徑的檔案名稱，就不會掃描含有此名稱的所有檔案 (無論路徑或所屬磁碟機爲何)。

新增

藉由這個按鈕，您可以將輸入到輸入方塊中的檔案物件新增至顯示視窗。

刪除

此按鈕會從清單刪除選取的項目。如果沒有選取任何項目，此按鈕將無作用。

注意
如果您將完整的磁碟分割新增到檔案物件清單，只有直接儲存在磁碟分割底下的檔案不用接受掃描，但此規則不適用位於對應磁碟分割上子目錄中的檔案：
例如：要略過的檔案物件：`D:\ = D:\file.txt` 將排除在掃描程式的掃描範圍外，而 `D:\folder\file.txt` 不會排除在掃描範圍外。

13.1.1.3. 啓發式掃毒

此組態區段包含掃描引擎的啓發式掃毒設定。

AntiVir 產品內含威力非常強大的啓發式掃毒模組，可主動發現不明的惡意程式碼，亦即可在完成用來對抗破壞元素的特殊病毒簽章之前，並在病毒保護更新傳送之前先行制敵機先。病毒偵測作業牽涉到針對受影響的程式碼，深入分析並調查其中有無惡意程式碼的典型功能。如果掃描的程式碼表現出相關特徵，就會回報爲可疑。但這並不代表程式碼本身就是惡意程式碼。有時可能會出現誤判。使用者必須依據個人對於程式碼來源是否可信任的了解，決定如何處置受影響的程式碼。

巨集病毒啓發式掃毒

<u>巨集病毒啓發式掃毒</u>

您的 AntiVir 產品包含威力非常強大的病毒啓發式掃毒工具。此選項一經啓用，在修復期間，相關文件上的所有巨集都會被刪除，或者只是針對可疑的文件加以回報，亦即，您會收到警示。系統不只預設啓用此選項，也建議使用這個選項。

先進啓發式掃毒分析與偵測 (AHeAD)

<u>啓用 **AHeAD**</u>

您的 AntiVir 程式內含威力強大的 AntiVir AHeAD 啓發式掃毒技術，此技術可同時偵測不明 (新型態) 惡意程式碼。此選項一經啓用，您可以定義此啓發式掃毒技術的「積極」程度。""此選項會啓用爲預設值。

<u>低偵測等級</u>

此選項一經啓用，將可偵測到稍微不明的惡意程式碼，而在此情況下錯誤警示的機率並不高。

<u>中偵測等級</u>

如果您已選取使用此啓發式掃毒技術，這將會是預設選項。

<u>高偵測等級</u>

此選項一經啓用，將可偵測到極度不明的惡意程式碼，不過也更可能發生誤判。

13.1.2 報告

掃描程式包含完整的報告功能。因此，您可以取得指定掃描結果的準確資訊。報告檔案包含系統的所有項目，以及指定掃描的警示與訊息。

注意
爲確認在偵測到病毒或有害程式時，掃描程式已執行的相關動作，應該一律建立報告檔。

報告功能

<u>關閉</u>

此選項一經啓用，掃描程式就不會報告指定掃描的動作與結果。

<u>預設值</u>

此選項一經啓用，掃描程式會記錄相關檔案名稱與其路徑。此外，目前的掃描組態、版本資訊與被授權人的資訊，全都會寫入報告檔中。

<u>進階</u>

啓用此選項時，除了預設資訊以外，掃描程式還會記錄警示與秘訣。

<u>完整</u>

此選項一經啓用，掃描程式還會記錄所有掃描的檔案。此外，會將相關的所有檔案與警示和提示包含在報告檔中。

注意
如果您必須寄送報告檔給我們 (以便排解疑難)，請在此模式中建立此報告檔案。

13.2 Guard

組態的 [Guard] 區段負責即時掃描的組態。

13.2.1 掃描

通常您會想要持續監視系統。爲達到這個目的，請使用 Guard (= 即時掃描程式)。這樣您就可以針對病毒與有害程式，即時掃描電腦上所有複製或開啓的檔案。

掃描模式

此處可定義檔案的掃描時間。

讀取時掃描

此選項一經啓用，Guard 會在應用程式或作業系統讀取或執行檔案時，先行加以掃描。

寫入時掃描

此選項一經啓用，Guard 會在寫入檔案時先行掃描。您必須等候此處理序完成，才能再次存取檔案。

讀取與寫入時掃描

此選項一經啓用，Guard 會在開啓、讀取與執行檔案之前，並在寫入檔案之後掃描檔案。系統不只預設啓用此選項，也建議使用這個選項。

檔案

Guard 可以透過篩選器來專門掃描帶有特定副檔名 (類型) 的檔案。

所有檔案

此選項一經啓用，所有檔案 (不論其內容或副檔名爲何) 都會進行病毒或惡意程式的掃描。

注意
一旦啓用所有檔案選項，便無法選取 **[副檔名]** 按鈕。

智慧副檔名辨識

此選項一經啓用，此程式會自動選擇要掃描病毒或有害程式的檔案。這表示程式會依據檔案內容決定是否要加以掃描。此程序在速度上會比透過使用副檔名清單方式來得緩慢，不過卻比較安全，因爲並不只有針對特定副檔名才進行掃描。

注意
智慧副檔名辨識選項一經啓用，便無法選取 **[副檔名]** 按鈕。

使用副檔名清單

此選項一經啓用，只會掃描帶有指定副檔名的檔案。所有可能包含病毒與有害程式的檔案類型都會預先設定好。此清單可經由 "**[副檔名]**" 按鈕手動加以編輯。系統不只預設啓用此選項，也建議使用這個選項。

注意
此選項一經啓用，""而且您已從清單中刪除所有特定副檔名項目時，會在 **[副檔名]** 按鈕底下顯示 [無副檔名] 字樣。

副檔名

藉由此按鈕，會開啓一個對話方塊並顯示所有於 **"[使用副檔名清單]"** 模式中掃描的所有副檔名。系統會針對副檔名設定預設項目，不過您可以新增或刪除這些項目。

注意
請注意，副檔名清單會依版本不同而有所差異。

封存

掃描封存

此選項一經啓用，會掃描封存。壓縮檔案經過掃描之後，會解壓縮並重新掃描一遍。預設會停用此選項。封存掃描會受限於遞迴深度、要掃描的檔案數量以及封存大小。您可以設定最大遞迴深度、要掃描的檔案數量以及封存大小上限。

注意
由於此處理序會對電腦效能產生極大的需求，因此系統預設會停用此選項。通常我們建議使用指定掃描來檢查封存。

遞迴深度上限

掃描封存時，Guard 會使用遞迴掃描：封存內的封存在經過解壓縮之後，會掃描其中是否有病毒與有害程式式。您可以定義遞迴深度。預設與建議的遞迴深度爲 1 層：直接位於主封存的所有封存會經過掃描程序。

檔案數上限

掃描封存時，可以限制封存中要掃描的檔案數量上限。要掃描的預設與建議檔案數量上限值爲 10 個。

*大小上限 **(KB)***

掃描封存時，可以限制要解壓縮的封存大小上限。建議的標準值爲 1000 KB。

13.2.1.1. 偵測有所發現時採取的動作

偵測有所發現時採取的動作

您可以定義當偵測到病毒或有害程式時，Guard 要執行的動作。

互動式

此選項一經啓用，只要 Guard 偵測到病毒或有害的程式，就會出現桌面通知。您可以選擇移除偵測到的惡意程式碼，或經由 [詳細資料] 按鈕存取其他可能的病毒處理動作。這些動作會顯示在對話方塊中。這些動作將會顯示在對話方塊中。此選項會啓用爲預設值。

如需詳細資訊，按一下此處。

自動

此選項一經啓用，偵測到病毒時將不會出現任何對話方塊。Guard 會根據您在這個區段中預先定義爲主要和次要動作的設定來反應。

備份至隔離區

此選項一經啓用，Guard 會在執行要求的主要或次要動作之前建立備份複本。備份複本會儲存至隔離區。如果該項目具有參考價值，可以透過隔離區管理員加以還原。您也可以將備份複本傳送給 Avira 惡意程式碼研究中心。依物件特性，您可以在隔離區管理員中找到更多可用的選項。

主要動作

是 Guard 發現病毒或有害程式時優先執行的動作。如果選取了 "**[修復]** "選項，但卻無法修復受影響的檔案，便會執行在"**[次要動作]**" 底下選取的動作。

注意
[次要動作] 選項必須當您已選取 [修復] 設定 (位於 [主要動作] 底下) 時才能選取。

修復

此選項一經啓用，Guard 會自動修復受影響的檔案。如果 Guard 無法修復受影響的檔案，會執行在次要動作底下選取的動作。

注意
我們建議使用自動修復動作，不過這意味著 Guard 將修改工作站上的檔案。

刪除

此選項一經啓用，會刪除檔案。此處理序在速度上會比 [覆寫並刪除] 要來得快速。

覆寫並刪除

此選項一經啓用，Guard 會先使用預設模式來覆寫檔案，再加以刪除。此檔案無法還原。

重新命名

此選項一經啓用，Guard 會重新命名檔案。如此將無法再直接存取這些檔案 (例如按兩下滑鼠)。檔案可以在之後修復並重新賦予其原始名稱。

略過

此選項一經啓用，可允許存取檔案，並保留檔案原貌不動。

警告
工作站上受影響的檔案仍會繼續運作！此做法可能會對工作站造成嚴重的傷害！

拒絕存取

此選項一經啓用，報告功能必須已經啓用，Guard 才會將偵測項目輸入到報告檔案中。此外，此選項一經啓用，Guard 會將項目寫入事件記錄。

隔離區

此選項一經啓用，Guard 會將檔案移至隔離區。稍後可以修復此目錄中的檔案，必要時也可將其傳送至 Avira 惡意程式碼研究中心。

次要動作

"**[次要動作]**" 選項必須當您已選取 "**[修復]**" 選項 (位於 "**[主要動作]**" 底下) 時才能選取。透過這個選項，現在您可以決定要對無法修復的檔案採取哪些處置方式。

刪除

此選項一經啓用，會刪除檔案。此處理序在速度上會比 [覆寫並刪除] 要來得快速。

覆寫並刪除

此選項一經啓用，Guard 會先使用預設模式來覆寫檔案，再加以刪除。此檔案無法還原。

重新命名

此選項一經啓用，Guard 會重新命名檔案。如此將無法再直接存取這些檔案 (例如按兩下滑鼠)。檔案可以在之後修復並重新賦予其原始名稱。

略過

此選項一經啓用，可允許存取檔案，並保留檔案原貌不動。

警告
工作站上受影響的檔案仍會繼續運作！此做法可能會對工作站造成嚴重的傷害！

拒絕存取

此選項一經啓用，報告功能必須已經啓用，Guard 才會將偵測項目輸入到報告檔案中。此外，此選項一經啓用，Guard 會將項目寫入事件記錄。

隔離區

此選項一經啓用，Guard 會將檔案移至隔離區。稍後可以修復檔案，必要時也可將其傳送至 Avira 惡意程式碼研究中心。

注意
若您已選取 **[刪除]** 或 **[覆寫並刪除]** 做爲主要或次要動作，請注意下列事項：當啓發式掃毒模式偵測到病毒時，並不會刪除受影響的檔案，而是將之移至隔離區。

13.2.1.2. 進一步動作

通知

事件記錄

使用事件記錄

此選項一經啓用，每次偵測到病毒時，會將項目新增至 Windows 事件記錄。 您可以在 Windows 事件檢視器中呼叫這些事件。此選項會啓用爲預設值。

自動啓動

封鎖自動啓動功能

此選項一經啓用，包括 USB 隨身碟、CD 和 DVD 光碟機以及網路磁碟機在內，所有連線磁碟機的 Windows 自動啓動功能執行都會遭到封鎖。 啓用 Windows 自動啓動功能時，會在載入或連線時立即讀取資料媒體或網路磁碟機上的檔案，因此會自動啓動及複製檔案。這項功能附帶高度安全風險，不過，惡意程式碼和有害程式可能會隨著自動啓動而安裝。自動啓動功能對於 USB 隨身碟尤其重要，因爲隨身碟上的資料可能隨時會變更。

排除 **CD** 和 **DVD**

此選項一經啓用，CD 和 DVD 光碟機上允許自動啓動功能。

警告
務必只有在確定使用的是信任的資料媒體時，才停用 CD 和 DVD 光碟機的自動啓動功能。

13.2.1.3. 例外

透過這些選項，您可以設定 Guard (即時掃描) 的例外物件。這時進行即時掃描時就不會包含相關物件。Guard 可以透過要略過的處理序清單，在即時掃描期間忽略這些物件的檔案存取行爲。例如，使用資料庫或備份解決方案時，這種作法最有用。請在指定要略過的處理序和檔案物件時注意下列事項：此清單將由上而下進行處理。清單越長，每次處理存取的清單時，所需的處理器時間也會越久。因此，請盡可能將清單變短一點。

要讓 Guard 略過的處理序

此清單中處理序的所有檔案存取行爲，全都不會受到 Guard 的監視。

<u>輸入方塊</u>

在此欄位中，輸入要讓即時掃描略過的處理序名稱。預設不會輸入任何處理序。

注意
您最多可以輸入 128 個處理序。

注意
輸入處理序時，可接受 Unicode 符號。因此，您可以輸入名稱中包含特殊符號的處理序或目錄。

注意
您可以選擇不提供完整路徑詳細資料來設定排除 Guard 監視的處理序。
application.exe
不過這種作法僅適用於可執行檔位於硬碟的處理序。
請勿針對可執行檔位在動態磁碟機上的處理序指定任何例外。動態磁碟機可指定爲卸除式磁碟，例如 CD、DVD 或 USB 隨身碟等。

注意
磁碟機資訊必須採用下列格式輸入：[磁碟機代號]:\
磁碟機時只能用冒號 (:) 來指定。

注意
當指定處理序時，您可以使用萬用字元* (任何字元數目) 和 ?? (單一個字元)。
C:\Program Files\Application\application.exe
C:\Program Files\Application\applicatio?.exe
C:\Program Files\Application\applic*.exe
C:\Program Files\Application*.exe
爲了避免處理序遭全域性排除而不受 Guard 監控，包括下列字元的指定將排除爲無效：* (星號)、?(問號)、/ (斜線)、\ (反斜線)、.(點)、:(冒號)。

注意
指定的處理序路徑和檔案名稱長度上限爲 255 個字元。清單中的項目結果總數不得超過 6000 個字元。

警告
請注意，所有由清單中記錄之處理序存取的檔案，全部都會從病毒與有害程式的掃描作業中排除！無法排除 [Windows 檔案總管] 與作業系統本身。會忽略清單中對應的項目。



此按鈕會開啓新的視窗，供您選取可執行檔。

<u>處理序</u>

"**[處理序]**" 按鈕會開啓 " *[處理序選項]*" 視窗，顯示執行中的處理序。

<u>新增</u>

藉由這個按鈕，您可以將輸入到輸入方塊中的處理序新增至顯示視窗。

<u>刪除</u>

藉由這個按鈕，您可以從顯示視窗刪除選取的處理序。

要讓 Guard 略過的檔案物件

對此清單所列檔案物件的存取，全都不會受到 Guard 的監視。

<u>輸入方塊</u>

您可以在此方塊中輸入不要包含在即時掃描中的檔案物件名稱。預設不會輸入任何檔案物件。

注意
當指定要略過的檔案物件時，您可以使用萬用字元* (任何字元數目) 和 ?? (單一個字元)。也會排除個別副檔名 (內含萬用字元)：
C:\Directory*.mdb
*.mdb
*.md?
.xls
C:\Directory*.log

注意
目錄名稱必須以反斜線 (\) 結尾，否則會假定爲檔案名稱。

注意
清單上的項目總計不得超過 6000 個字元。

注意
如果排除目錄，會一併自動排除所有子目錄。

注意
針對每個磁碟機，透過輸入完整路徑 (以磁碟機代號開頭)，最多可指定 20 個例外。
例如：C:\Program Files\Application\Name.log

不含完整路徑的例外上限爲 64。
例如：*.log

注意
萬一已經有動態磁碟機在其他磁碟上裝載爲目錄，就必須在例外清單中使用整合的磁碟作業系統別名：
例如，\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
假如您使用裝載點 (例如，C:\DynDrive)，還是會掃描動態磁碟。您可以從 Guard 的報告檔中判斷要使用的作業系統別名。



此按鈕會開啓新的視窗，供您選取要排除的檔案物件。

<u>新增</u>

藉由這個按鈕，您可以將輸入到輸入方塊中的檔案物件新增至顯示視窗。

<u>刪除</u>

藉由這個按鈕，您可以從顯示視窗刪除選取的檔案物件。

請在指定例外時注意下列更多事項：

注意
爲了排除使用簡短 DOS 檔名 (8.3 DOS 名稱慣例) 存取的物件，還必須在清單中輸入相關的簡短檔名。

注意
內含萬用字元的檔名不可以反斜線來結束。

例如：

```
C:\Program Files\Application\applic*.exe\
```

此項目無效，且不會被視爲例外！

注意
您可以在 Guard 報告檔中找到 Guard 用來掃描受感染檔案的路徑。請在例外清單中清楚指出相同的路徑。請如以下所示進行：將 Guard 的通訊協定功能設爲 **[完整]** (於組態的 Guard::Report)接著在 Guard 已啓用的狀態下，存取檔案、資料夾、裝載的磁碟機。現在您可以從 Guard 報告檔中讀取要使用的路徑。報告檔案存取路徑爲控制中心的本機保護::Guard。

將予以排除處理序的範例：

– application.exe

這個 application.exe 處理序會指定排除不進行 Guard 掃描，不管其位處在哪一個硬碟和哪一個目錄中。

– C:\Program Files1\Application.exe

位在路徑 C:\Program Files1 下面之檔案 application.exe 的處理序，將排除不進行 Guard 掃描。

– C:\Program Files1*.exe

位在路徑 C:\Program Files1 下面的可執行檔的所有處理序，將排除不進行 Guard 掃描。

將予以排除檔案的範例：

– *.mdb

副檔名爲 'mdb' 的所有檔案都將排除不進行 Guard 掃描

– *.xls*

副檔名開頭爲 'xls' 的所有檔案都將排除不進行 Guard 掃描，例如副檔名 爲 .xls 和 .xlsx 的檔案。

– C:\Directory*.log

副檔名爲 'log' 且位在路徑 C:\Directory 下的任何記錄檔，都將排除不進行 Guard 掃描。

-

13.2.1.4. 啓發式掃毒

此組態區段包含掃描引擎的啓發式掃毒設定。

AntiVir 產品內含威力非常強大的啓發式掃毒模組，可主動發現不明的惡意程式碼，亦即可在完成用來對抗破壞元素的特殊病毒簽章之前，並在病毒保護更新傳送之前先行制敵機先。病毒偵測作業牽涉到針對受影響的程式碼，深入分析並調查其中有無惡意程式碼的典型功能。如果掃描的程式碼表現出相關特徵，就會回報爲可疑。但這並不代表程式碼本身就是惡意程式碼。有時可能會出現誤判。使用者必須依據個人對於程式碼來源是否可信任的了解，決定如何處置受影響的程式碼。

巨集病毒啓發式掃毒

<u>巨集病毒啓發式掃毒</u>

您的 AntiVir 產品包含威力非常強大的病毒啓發式掃毒工具。此選項一經啓用，在修復期間，相關文件上的所有巨集都會被刪除，或者只是針對可疑的文件加以回報，亦即，您會收到警示。系統不只預設啓用此選項，也建議使用這個選項。

先進啓發式掃毒分析與偵測 (AHeAD)

<u>啓用 **AHeAD**</u>

您的 AntiVir 程式內含威力強大的 AntiVir AHeAD 啓發式掃毒技術，此技術可同時偵測不明 (新型態) 惡意程式碼。此選項一經啓用，您可以定義此啓發式掃毒技術的「積極」程度。""此選項會啓用爲預設值。

<u>低偵測等級</u>

此選項一經啓用，將可偵測到稍微不明的惡意程式碼，而在此情況下錯誤警示的機率並不高。

<u>中偵測等級</u>

如果您已選取使用此啓發式掃毒技術，這將會是預設選項。

<u>高偵測等級</u>

此選項一經啓用，將可偵測到極度不明的惡意程式碼，不過也更可能發生誤判。

13.2.2 ProActive

Avira AntiVir ProActiv 保護您免於尙無病毒定義或啓發式掃毒的不明新威脅。ProActiv 技術整合至 Guard 元件，會觀察及分析程式所執行的動作。程式的行爲對照典型惡意程式碼的動作模式進行檢查：動作類型和動作順序。如果程式表現出惡意程式碼的典型行爲，就會被視爲病毒偵測 ：您可以選擇封鎖程式或忽略通知並繼續使用程式。您可以將程式歸類爲信任的程式，並將它加入至許可程式的應用程式篩選器。您也可以選擇使用 *[永遠封鎖]* 命令，將程式加入至封鎖程式的應用程式篩選器。

ProActiv 元件使用 Avira 惡意程式碼研究中心開發的規則集，來識別可疑行爲的典型行爲。此規則集由 Avira GmbH 資料庫提供。Avira AntiVir ProActiv 會將偵測到任何可疑程式的資訊傳送至 Avira 資料庫以供記錄。您可以選擇停用對 Avira 資料庫的資料傳輸。

注意
ProActiv 技術仍無法用於 64 位元系統！Windows 2000 不支援 ProActiv 元件。

一般

<u>啓用 **Avira AntiVir ProActiv**</u>

此選項一經啓用，在電腦系統上的程式就會受到監視並檢查其是否有可疑行爲。偵測到典型的惡意程式碼行爲時，您會收到訊息。您可以封鎖程式或選擇 "*[略過]*" 繼續使用程式。監視程序排除： 歸類爲信任的程式、許可的應用程式篩選器中預設包含的信任且已簽署的程式，以及您已加入至許可程式的應用程式篩選器中的所有程式。

<u>參與 **AntiVir ProActiv** 社群提高電腦的'安全性。</u>

此選項一經啓用，Avira AntiVir ProActiv 會傳送有關可疑程式的資料，並在特定情況下，將可疑程式的檔案 (可執行檔) 傳送到 Avira 惡意程式碼研究中心進行更進一步的線上掃描。評估後，此資料會加入至 ProActiv 行爲分析規則集。如此，您便成爲 Avira ProActiv 社群的一份子，對 ProActiv 資訊安全技術的持續改善和精進有所貢獻。 此選項一經停用，就不會傳送任何資料，但不影響 ProActiv 功能。

<u>如需詳細資訊，請按一下這裡。</u>

您可以透過這個連結存取網頁，取得有關進階線上掃描的詳細資訊。這張網際網路頁面包含了在進階線上掃描時所傳輸的任何資料。

13.2.2.1. 應用程式篩選器：要封鎖的應用程式

在 *[應用程式篩選器: 要封鎖的應用程式]* 底下，您可以輸入歸類爲有害的程式以及 Avira AntiVir ProActiv 預設會封鎖的應用程式。加入的應用程式無法在電腦系統上執行。您也可以經由 Guard 可疑程式式行爲通知，透過選取 *[永遠封鎖此程式]* 選項，將程式加入至封鎖應用程式篩選器。

要封鎖的應用程式

應用程式

此清單包含您經由組態輸入或是經由通知 ProActiv 元件而歸類爲有害程式的所有應用程式。清單上的應用程式遭到 Avira AntiVir ProActiv 封鎖，無法在電腦系統上執行。當封鎖的程式啓動時，會出現作業系統訊息。Avira AntVir ProActiv 依據指定的路徑和檔案名稱來識別封鎖的應用程式，封鎖時不考慮內容。

<u>輸入方塊</u>

在此方塊中輸入您要封鎖的應用程式。必須指定完整路徑、檔案名稱和副檔名來識別應用程式。路徑必須顯示應用程式所在的磁碟機或以環境變數開頭。



此按鈕會開啓新的視窗，供您選取要封鎖的應用程式。

<u>新增</u>

您可以使用 "**[新增]**" 按鈕，將在輸入方塊中指定的應用程式轉移至要封鎖的應用程式清單。

注意
無法加入作業系統正常運作所需的應用程式。

<u>刪除</u>

The "**[刪除]**" 按鈕讓您從要封鎖的應用程式清單中移除反白的應用程式。

13.2.2.2. 應用程式篩選器：許可的應用程式

[應用程式篩選器:許可的應用程式] 區段列出 ProActive 元件不監視的應用程式：歸類爲信任且預設包含在清單中的已簽署程式、歸類爲信任且已加入至應用程式篩選器中的所有應用程式： 您可以在 [組態] 將許可的應用程式加入至清單。也可以選擇使用 Guard 通知中的 **[信任的程式]** 選項，經由 Guard 通知將應用程式加入至可疑程式行爲。

要略過的應用程式

應用程式

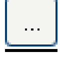
此清單包含 ProActive 元件不監視的應用程式。在預設安裝設定中，此清單包含來自受信任供應商的已簽署應用程式。您可以選擇在組態或 Guard 通知中加入視爲受信任的應用程式。ProActiv 元件使用路徑、檔案名稱和內容來識別應用程式。建議您檢查程式內容，因爲惡意程式碼可透過變更 (例如更新程式) 加入至程式。您可以從指定的類型，決定是否應該執行內容檢查：如果是 *[內容]* 類型，ProActiv 元件監視作業排除依路徑和檔案名稱指定的應用程式之前，會先檢查檔案內容是否變更。如果檔案內容已修改，ProActive 元件會重新監視應用程式。如果是 "*[路徑]*" 類型，Guard 監視作業排除應用程式之前，不會執行內容檢查。若要變更排除類型，請按一下顯示的類型。

警告
請僅在例外情況下才使用 *[路徑]* 類型。因爲惡意程式碼可透過更新加入至應用程式，原本無害的應用程式現在就會成爲惡意程式碼。

注意
即使不包含在清單中，有些信任的應用程式預設不受 ProActiv 元件監視，例如包括您的 AntiVir 的所有應用程式元件。

輸入方塊

在此方塊中輸入 ProActive 元件監視作業要排除的應用程式。必須指定完整路徑、檔案名稱和副檔名來識別應用程式。路徑必須顯示應用程式所在的磁碟機或以環境變數開頭。



此按鈕會開啓新的視窗，供您選取要排除的應用程式。

新增

您可以使用 "**[新增]**" 按鈕，將在輸入方塊中指定的應用程式轉移至要排除的應用程式清單。

刪除

The "**[刪除]**" 按鈕讓您從要排除的應用程式清單中移除反白的應用程式。

13.2.3 報告

Guard 包含延伸的記錄功能，提供使用者或系統管理員有關偵測類型與方法的準確記錄。

報告功能

此群組可決定報告檔案內容。

關閉

此選項一經啓用，Guard 便不會建立記錄。
建議您只有在例外情況下才關閉記錄功能，例如當您對多個病毒或有害程式執行試用版軟體時。

預設值

此選項一經啓用，Guard 會將重要的資訊 (有關病毒偵測、警示與錯誤事項) 記錄到報告檔中，並忽略較不重要的資訊，讓報告更爲簡明易懂。此選項會啓用爲預設值。

進階

此選項一經啓用，Guard 會將較不重要的資訊同時包含在報告檔中。

完整

此選項一經啓用，Guard 會將所有可用資訊記錄到報告檔中，包括檔案大小、檔案類型、日期等等。

限制報告檔

將大小限制爲

此選項一經啓用，可將報告檔大小限定爲特定大小。可能的值如下：允許介於 1 到 100 MB 之間的值。當限制報告檔大小以節省系統資源時，允許使用約 50 KB 的額外空間。如果記錄檔大小超出指定大小 50 KB 以上，會先刪除舊的項目，直到達到指定大小減去 50 KB。

縮短報告前先備份

此選項一經啓用，縮短報告檔案前會先加以備份。

在報告檔中寫入組態

此選項一經啓用，會將即時掃描的組態記錄在報告檔中。

注意
如果您尚未指定任何報告檔限制，當此報告檔達到 100MB 時，新的報告檔會自動建立。舊報告的備份隨即建立。最多可儲存 3 個舊報告檔案的備份。最舊的備份會最先遭到刪除。

13.3 MailGuard

[組態] 的 [MailGuard] 區段負責 MailGuard 的組態。

13.3.1 掃描

使用 MailGuard 來掃描內送電子郵件中的病毒、惡意程式碼與垃圾郵件。外寄的電子郵件可以使用 MailGuard 來掃描其中的病毒與惡意程式碼。電腦上由不明的傀儡程式所寄發的垃圾郵件可由 MailGuard 加以封鎖以防堵垃圾郵件。

掃描

開啓 MailGuard

此選項一經啓用，電子郵件流量將受 MailGuard 監控。MailGuard 是一種 Proxy 伺服器，會檢查您所使用的電子郵件伺服器和電腦系統上電子郵件用戶端程式之間的資料流量：內送電子郵件會按預設掃描是否有惡意程式碼。 此選項一經停用，MailGuard 服務仍爲啓動狀態，但是由 MailGuard 的監控作業會停用。

掃描內送電子郵件

此選項一經啓用，會掃描內送電子郵件中是否有病毒與惡意程式碼以及垃圾郵件。MailGuard 支援 POP3 和 IMAP 通訊協定。啓用電子郵件用戶端所使用的收件匣帳戶，接收由 MailGuard 監視的電子郵件。

監視 POP3 帳號

此選項一經啓用，會在指定的連接埠上監視 POP3 帳戶。

監視的連接埠

請在此欄位中，輸入 POP3 通訊協定要當做收件匣使用的連接埠。個別連接埠可用逗號來分隔。

預設值

此按鈕會將指定的連接埠重設爲預設的 POP3 連接埠。

監視 IMAP 帳號

此選項一經啓用，會在指定的連接埠上監視 IMAP 帳戶。

監視的連接埠

請在此欄位中，輸入 IMAP 通訊協定要當做收件匣使用的連接埠。個別連接埠可用逗號來分隔。

預設值

此按鈕會將指定的連接埠重設爲預設的 IMAP 連接埠。

掃描外寄電子郵件 (SMTP)

此選項一經啓用，會掃描外寄的電子郵件中是否有病毒與惡意程式碼。由不明傀儡程式所寄發的垃圾郵件會遭到封鎖。

監視的連接埠

請在此欄位中，輸入 SMTP 通訊協定要當做寄件匣使用的連接埠。個別連接埠可用逗號來分隔。

預設值

此按鈕會將指定的連接埠重設爲預設的 SMTP 連接埠。

> 注意
> 若要確認使用的通訊協定與連接埠，請開啓電子郵件用戶端程式中的電子郵件帳戶內容。正常情況下會使用預設連接埠。

13.3.1.1. 偵測有所發現時採取的動作

此組態區段內含當 MailGuard 在電子郵件或附件中發現病毒或有害程式時，所要採取的動作設定。

注意
這些動作會同時在內送與外寄的電子郵件中偵測到病毒時執行。

偵測有所發現時採取的動作

互動式

此選項一經啓用，一旦在電子郵件或附件中偵測到病毒或有害程式時會顯示對話方塊，供您選擇對相關電子郵件或附件的處置方式。此選項會啓用爲預設值。

顯示進度列

此選項一經啓用，MailGuard 會在電子郵件下載期間顯示進度列。只有當 **[互動式]** 選項已經選取時，才會啓用此選項。

自動

此選項一經啓用，發現病毒或有害程式時便不會再通知您。MailGuard 會依據您在此區段定義的設定來因應。

主要動作

主要動作是 MailGuard 在電子郵件中發現病毒或有害程式時優先執行的動作。"**[略過電子郵件]**" 選項一經選取，就可以同時在 "**[受影響的附件]**" 底下選取當偵測到附件中的病毒或有害程式時要用來處理的程序。

刪除電子郵件

此選項一經啓用，當偵測到病毒或有害程式時，會自動刪除受影響的電子郵件。電子郵件本文會以如下所示的預設內容來取代。此規則同樣適用所有包含的附件；這些附件會同時以預設內容來取代。

隔離電子郵件

此選項一經啓用，當偵測到病毒或有害程式時，完整的電子郵件 (包括所有附件) 將放到隔離區。日後必要時，可以將它還原。受影響的電子郵件本身會刪除。電子郵件本文會以如下所示的預設內容來取代。此規則同樣適用所有包含的附件；這些附件會同時以預設內容來取代。

略過電子郵件

此選項一經啓用，即使偵測到病毒或有害程式，都會略過受影響的電子郵件。不過，您可以決定要如何處置受影響的附件：

受影響的附件

"**[受影響的附件]**" 選項必須當您已經選取 "**[略過電子郵件]**" 設定 (位於 "**[主要動作]**" 底下) 時才能選取。透過這個選項，現在您可以決定當偵測到附件中的病毒或有害程式時，要執行的動作。

刪除

此選項一經啓用，當偵測到病毒或有害程式時，會將受影響的附件刪除並以預設內容加以取代。

隔離

此選項一經啓用，會將受影響的附件置放到隔離區並加以刪除 (以預設內容來取代)。若有需要，受影響的附件可於稍後復原。

略過

此選項一經啓用，即使偵測到病毒或有害程式，都會略過並遞送附件。

警告
此選項一經選取，MailGuard 便無法保護您免於病毒或有害程式的侵擾。只有當您很清楚自己的行爲有何後果時才選取此項目。請停用電子郵件程式中的預覽功能，而且絕對不要按兩下附件加以開啓！

13.3.1.2. 其他動作

此組態區段內含當 MailGuard 在電子郵件或附件中發現病毒或有害程式時，所要採取的其他動作設定。

注意
這些動作只有在內送的電子郵件中偵測到病毒時才會執行。

刪除或移動電子郵件時顯示的預設文字

此方塊中的內容會插入到電子郵件中 (而非受影響的電子郵件中) 並當成郵件傳送出去。您可以編輯此訊息。內容長度上限爲 500 個字元。

您可以使用下列按鍵組合來格式化郵件：

Strg + Enter 插入換行符號。

預設值

此按鈕會將預先定義的預設內容插入編輯方塊中。

刪除或移動附件時顯示的預設文字

此方塊中的內容會插入到電子郵件中 (而非受影響的附件中) 並當成郵件傳送出去。您可以編輯此訊息。內容長度上限爲 500 個字元。

您可以使用下列按鍵組合來格式化郵件：

Strg + Enter 插入換行符號。

預設值

此按鈕會將預先定義的預設內容插入編輯方塊中。

13.3.1.3. 啓發式掃毒

此組態區段包含掃描引擎的啓發式掃毒設定。

AntiVir 產品內含威力非常強大的啓發式掃毒模組，可主動發現不明的惡意程式碼，亦即可在完成用來對抗破壞元素的特殊病毒簽章之前，並在病毒保護更新傳送之前先行制敵機先。病毒偵測作業牽涉到針對受影響的程式碼，深入分析並調查其中有無惡意程式碼的典型功能。如果掃描的程式碼表現出相關特徵，就會回報爲可疑。但這並不代表程式碼本身就是惡意程式碼。有時可能會出現誤判。使用者必須依據個人對於程式碼來源是否可信任的了解，決定如何處置受影響的程式碼。

巨集病毒啓發式掃毒

啓用巨集病毒啓發式掃毒

您的 AntiVir 產品包含威力非常強大的病毒啓發式掃毒工具。此選項一經啓用，在修復期間，相關文件上的所有巨集都會被刪除，或者只是針對可疑的文件加以回報，亦即，您會收到警示。系統不只預設啓用此選項，也建議使用這個選項。

先進啓發式掃毒分析與偵測 (AHeAD)

啓用 **AHeAD**

您的 AntiVir 程式內含威力強大的 AntiVir AHeAD 啓發式掃毒技術，此技術可同時偵測不明 (新型態) 惡意程式碼。此選項一經啓用，您可以定義此啓發式掃毒技術的「積極」程度。""此選項會啓用爲預設值。

低偵測等級

此選項一經啓用，將可偵測到稍微不明的惡意程式碼，而在此情況下錯誤警示的機率並不高。

中偵測等級

如果您已選取使用此啓發式掃毒技術，這將會是預設選項。系統不只預設啓用此選項，也建議使用這個選項。

高偵測等級

此選項一經啓用，將可偵測到極度不明的惡意程式碼，不過也更可能發生誤判。

13.3.1.4. AntiBot

MailGuard 的 AntiBot 功能可防止您的電腦變成所謂傀儡網路的一部分，並被用來散播垃圾電子郵件：爲了透過傀儡網路來散播垃圾郵件，攻擊者通常會使用傀儡程式 (Bot) 來感染一群電腦，並透過這個傀儡程式連線至 IRC 伺服器、開啓特定的通道，然後等候發送垃圾郵件的命令。爲了區分由不明傀儡電腦所寄發的垃圾電子郵件與正常電子郵件，MailGuard 會檢查外寄電子郵件的 SMTP 伺服器與寄件者是否包含在許可的伺服器與寄件者清單中。如果與預期不符，則會封鎖外寄的電子郵件，亦即不會寄發電子郵件。封鎖的電子郵件會顯示在對話方塊中。

注意
只有當 MailGuard 啓用爲掃描外寄電子郵件，才能使用 AntiBot 功能 (請參閱 **[掃描外寄電子郵件]** 選項 (於 MailGuard ::掃描) 底下)。

許可的伺服器

MailGuard 會授權此清單中的所有伺服器來寄送電子郵件：傳送至這些伺服器的電子郵件**不會**遭到 MailGuard 封鎖。如果清單中沒有任何伺服器，就不會掃描用來傳送外寄電子郵件的 SMTP 伺服器。如果清單中有伺服器，MailGuard 會封鎖未列在清單中的所有 SMTP 伺服器所寄出的電子郵件。

輸入方塊

請在此方塊中，輸入要用來寄送電子郵件的 SMTP 伺服器主機名稱或 IP 位址。

注意
您可以在電子郵件程式中當初建立使用者帳戶的日期底下，找到電子郵件程式用來傳送電子郵件的 SMTP 伺服器詳細資料。

新增

您可以使用這個按鈕，將輸入方塊中指定的伺服器納入許可的伺服器清單中。

刪除

此按鈕會從許可的伺服器清單中，刪除反白的項目。如果沒有選取任何項目，此按鈕將無作用。

全部清除

此按鈕會從許可的伺服器清單中，刪除所有項目。

許可的寄件者

MailGuard 會授權此清單中的所有寄件者來寄送電子郵件：由此電子郵件地址所寄出的電子郵件，**不會**遭到 MailGuard 封鎖。如果清單中沒有任何寄件者，就不會掃描用來傳送外寄電子郵件的電子郵件地址。如果清單中有寄件者，MailGuard 會封鎖未列在清單中的所有寄件者所寄出的電子郵件。

輸入方塊

請在此方塊輸入您的電子郵件寄件者地址。

新增

您可以使用這個按鈕，將輸入方塊中指定的寄件者納入許可的寄件者清單中。

刪除

此按鈕會從許可的寄件者清單中，刪除反白的項目。如果沒有選取任何項目，此按鈕將無作用。

全部清除

此按鈕會從許可的寄件者清單中，刪除所有項目。

13.3.2 一般

13.3.2.1. 例外

掃描例外

此表會顯示排除在 AntiVir MailGuard 掃描範圍外的電子郵件地址清單 (白名單)。

> 注意
> MailGuard 會針對內送電子郵件，獨佔使用例外清單。

狀態

圖示	**Description**
	不會再掃描此電子郵件地址來尋找垃圾郵件。
	不會再掃描此電子郵件地址來尋找惡意程式碼。
	不會再掃描此電子郵件地址來尋找惡意程式碼或垃圾郵件。

電子郵件地址

不會再掃描的電子郵件。

惡意程式碼

此選項一經啓用，就不會再掃描該電子郵件地址來尋找惡意程式碼。

垃圾郵件

此選項一經啓用，就不會再掃描該電子郵件地址來尋找垃圾郵件。

上移

您可以使用此按鈕，將反白的電子郵件地址上移至較高的位置。如果沒有反白的項目，或者反白的地址已經列在清單首位，此按鈕就不會啓用。

下移

您可以使用此按鈕，將反白的電子郵件地址下移至較低的位置。如果沒有反白的項目，或者反白的地址已經列在清單末尾，此按鈕就不會啓用。

輸入方塊

您可以在此方塊中，輸入要新增至不接受掃描的電子郵件地址清單中的電子郵件地址。依據您的設定，MailGuard 日後將不再掃描這些電子郵件地址。

注意
輸入電子郵件地址時，您可以使用萬用字元：* 用於任何數量的字元，而 **?** 僅用於單一字元。不過，您可以專門針對不接受垃圾郵件掃描的電子郵件地址使用萬用字元。如果您藉由勾選 **[惡意程式碼]** 排除清單方塊，嘗試從惡意程式碼掃描中排除包含萬用字元的地址，會收到錯誤訊息。請注意，當您輸入包含萬用字元的地址時，指定的字元順序必須與電子郵件地址結構相符 (*@*.*)。

警告
使用萬用字元時，請參考提供的範例。請選擇性使用萬用字元，並注意要將哪些包含萬用字元的電子郵件地址納入垃圾郵件白名單中。

例如：在電子郵件地址中使用萬用字元 (垃圾郵件白名單)

- `virus@avira.* /` = 所有帶有此地址的電子郵件以及任何頂層網域：virus@avira.de、virus@avira.com、virus@avira.net 等等。
- `*@avira.com` = 所有來自 **avira.com** 網域的電子郵件：info@avira.com、virus@avira.com、contakt@avira.com、employee@avira.com
- `info@*.com` = 所有包含頂層網域 **com** 以及地址**資訊**的電子郵件地址：第二層網域可以是任何名稱：info@name1.com、info@name2.com 等等。

新增

透過這個按鈕，您可以將輸入方塊中所輸入的電子郵件地址新增至不要掃描的電子郵件地址清單中。

刪除

此按鈕會從清單中刪除反白的電子郵件地址。

匯入 **Outlook** 通訊錄

透過這個按鈕，您可以從 MS Outlook 電子郵件程式的通訊錄中，將電子郵件地址匯入例外清單中。匯入的電子郵件地址便不會經過垃圾郵件掃描。

匯入 **Outlook Express** 通訊錄

透過這個按鈕，您可以從 MS Outlook Express 電子郵件程式的通訊錄中，將電子郵件地址匯入例外清單中。匯入的電子郵件地址便不會經過垃圾郵件掃描。

13.3.2.2. 快取

快取

MailGuard 快取包含掃描的電子郵件相關資料，並以統計資料形式顯示在控制中心的 MailGuard 底下。內送電子郵件的副本同時也會寄存在快取中。反垃圾郵件模組的訓練功能也可使用這些電子郵件 (良好的電子郵件 – 用於訓練、垃圾電子郵件 – 用於訓練)。

注意
您必須啓用反垃圾郵件模組以便將內送電子郵件備份到快取中。

存放在快取區中的電子郵件數目上限

此欄位可用來設定 MailGuard 要存放在快取中的電子郵件數量上限。日期最早的電子郵件會最先遭到刪除。

電子郵件儲存天數上限

您可在此方塊中，輸入電子郵件儲存天數上限。過了這段時間，就會從快取移除電子郵件。

清空快取

按一下此按鈕以刪除存放在快取中的電子郵件。

13.3.2.3. MailGuard

反垃圾郵件

AntiVir MailGuard 服務會檢查電子郵件與其中的附件有無病毒與有害的程式。此外，它能可靠地保護您免於垃圾電子郵件的騷擾。

反垃圾郵件

啓用反垃圾郵件模組

啓用此選項，會連帶啓用 MailGuard 的反垃圾郵件功能。

標記電子郵件主旨

此選項一經啓用，一旦偵測到垃圾電子郵件，就會在原始主旨行中加上註解。

簡易

收到垃圾郵件或網路釣魚郵件時，會新增 [垃圾郵件] 或 [網路釣魚] 的附錄。此選項會啓用爲預設值。

詳細

屬於網路釣魚性質的垃圾郵件主旨行會加上一段前置詞，以提醒收件者注意該郵件可能爲垃圾郵件。

啓用記錄功能

此選項一經啓用，MailGuard 會建立特殊的反垃圾郵件報告檔。

使用即時黑名單

此選項一經啓用，會即時查詢所謂的「黑名單」，並透過此名單所提供的額外資訊來判斷來源可疑的電子郵件是否爲垃圾郵件。""

逾時:n 秒

如果在經過 n 秒之後黑名單仍舊無法提供相關資訊，則會中止查詢黑名單的嘗試動作。

清除訓練資料庫

按一下此按鈕以刪除訓練資料庫。

自動將外寄郵件的收件者新增至白名單

此選項一經啓用，外寄電子郵件的收件者地址會自動新增至垃圾郵件白名單中 (此名單爲不需接受垃圾郵件掃描的電子郵件清單，定義於 **MailGuard::[一般] ::[例外]** 底下)。來自垃圾郵件白名單上地址的內送電子郵件，不會接受垃圾郵件掃描。不過，這些郵件會接受病毒與惡意程式碼掃描。預設會停用此選項。

注意
只有當 MailGuard 啓用爲掃描外寄電子郵件，才能啓用這個選項 (請參閱 **[掃描外寄電子郵件]** 選項 (位於 MailGuard ::掃描) 底下)。

13.3.2.4. 頁尾

您可以在 *[頁尾]* 底下設定所傳送的電子郵件中顯示的電子郵件頁尾。這項功能需要啓用外寄電子郵件的 MailGuard 掃描功能 (請參閱組態::MailGuard::掃描底下的 *[掃描外寄電子郵件 (SMTP)]* 選項)。您可以使用定義的 AntiVir MailGuard 頁尾，確認病毒防護程式已掃描傳送的電子郵件。您也可以選擇插入使用者定義頁尾文字。如果同時使用兩個頁尾選項，使用者定義文字會置於 AntiVir MailGuard 頁尾之後。

要傳送的電子郵件頁尾

附加 **AntiVir MailGuard** 頁尾

此選項一經啓用，就會在外寄電子郵件的訊息文字底下顯示 AntiVir MailGuard 頁尾。AntiVir MailGuard 頁尾確認傳送的電子郵件已通過 AntiVir MailGuard 病毒和有害程式掃描，而且不是源自不明的傀儡程式。AntiVir MailGuard 頁尾包含下列文字：「已使用 AntiVir MailGuard 掃描 [產品版本] [搜尋引擎的縮寫和版本編號] [病毒定義檔的縮寫和版本編號]」。

附加此頁尾

此選項一經啓用，您在輸入方塊中插入的文字就會在傳送的電子郵件中顯示爲頁尾。

輸入方塊

您可以在此輸入方塊插入文字，這些文字就會在傳送的電子郵件中顯示爲頁尾。

13.3.3 報告

MailGuard 包含延伸的記錄功能，提供使用者或系統管理員有關偵測類型與方法的準確記錄。

報告功能

此群組可決定報告檔案內容。

關閉

此選項一經啓用，MailGuard 便不會建立記錄。
建議您只有在例外情況下才關閉記錄功能，例如當您對多個病毒或有害程式執行試用版軟體時。

預設值

此選項一經啓用，MailGuard 會將重要的資訊 (有關病毒偵測、警示與錯誤事項) 記錄到報告檔中，並忽略較不重要的資訊，讓報告更爲簡明易懂。此選項會啓用爲預設值。

進階

此選項一經啓用，MailGuard 會將較不重要的資訊同時包含在報告檔中。

完整

此選項一經啓用，MailGuard 會將所有資訊全部包含在報告檔中。

限制報告檔

將大小限制爲

此選項一經啓用，可將報告檔大小限定爲特定大小。可能的值如下：允許介於 1 到 100 MB 之間的值。當限制報告檔大小以節省系統資源時，允許使用約 50 KB 的額外空間。如果記錄檔大小超出指定大小 50 KB 以上，會先刪除舊的項目，直到達到指定大小減去 50 KB。

縮短報告前先備份

此選項一經啓用，縮短報告檔案前會先加以備份。

在報告檔中寫入組態

此選項一經啓用，會將 MailGuard 組態記錄在報告檔中。

注意
如果您尚未指定任何報告檔限制，當此報告檔達到 100MB 時，新的報告檔會自動建立。舊報告的備份隨即建立。最多可儲存 3 個舊報告檔案的備份。最舊的備份會最先遭到刪除。

13.4 防火牆

[組態] 的 [FireWall] 區段負責 Avira FireWall 的組態。

13.4.1 介面卡規則

在 Avira FireWall 中，介面卡指的是模擬硬體裝置 (例如，miniport、橋接器連線等) 的軟體或是真實硬體裝置 (例如網路卡)。

Avira FireWall 會針對電腦上已安裝驅動程式的所有現有介面卡顯示其介面卡規則。

預先定義的介面卡規則取決於安全性等級。您可以在控制中心的線上保護 :: FireWall 設定中變更安全性等級。您可以在控制中心變更 FireWall 設定，或是定義您自己的介面卡規則。如果您已在控制中心的 FireWall 區段定義了自己的介面卡規則，安全性等級就會設爲「自訂」。

注意
所有預先定義之 Avira FireWall 規則的預設安全性等級設定都是 **[中]**。

ICMP 通訊協定

網際網路控制訊息通訊協定 (ICMP) 可用來交換網路上的錯誤與資訊訊息。此通訊協定也可搭配 ping 或 tracer 命令使用以顯示狀態訊息。
有了這項規則，您可以定義傳入與傳出的已封鎖訊息類型、洪水攻擊時的行為，以及 ICMP 分段封包的反應。此規則可用來防止所謂的 ICMP 洪水攻擊，但是由於它會回應每一個封包，因此會導致遭受攻擊的電腦 CPU 負載增加。

預先定義的 **ICMP** 通訊協定規則

設定：低	設定：中	設定：高
封鎖的傳入類型：**無類型**。 封鎖的傳出類型：**無類型**。 如果封包之間的延遲小於 **50** 毫秒，即假設為洪水攻擊。 **拒絕**分段的 ICMP 封包。	低等級適用相同規則。	封鎖的傳入類型：**數種類型** 封鎖的傳出類型：**數種類型** 如果封包之間的延遲小於 **50** 毫秒，即假設為洪水攻擊。 **拒絕**分段的 ICMP 封包。

封鎖的傳入類型：無類型/數種類型

只要在連結上按一下滑鼠，就會立即顯示 ICMP 封包類型清單。您可以透過這份清單，指定要封鎖的傳入 ICMP 訊息類型。

封鎖的傳出類型：無類型/數種類型

只要在連結上按一下滑鼠，就會立即顯示 ICMP 封包類型清單。您可以透過這份清單，選取要封鎖的傳出 ICMP 訊息類型。

洪水攻擊

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您輸入允許的 ICMPA 延遲上限。

分段的 **ICMP** 封包

只要在連結上按一下滑鼠，就可選擇拒絕或是不拒絕分段的 ICMP 封包。

TCP 連接埠掃描

有了這項規則，您就可以定義何時 FireWall 會認定為 TCP 連接埠掃描，以及在這種情況下需要採取的行動為何。此規則可用來預防所謂的 TCP 連接埠掃描攻擊，這種攻擊會偵測電腦上開放的 TCP 連接埠。此類攻擊會搜尋電腦上的弱點，並且經常伴隨著更危險的攻擊類型。

預先定義的 **TCP** 連接埠掃描規則

設定：低	設定：中	設定：高
如果在 **5,000** 毫秒內，掃描了 **50** 個 (含) 以上的連接埠，即假設為 TCP 連接埠	如果在 **5,000** 毫秒內，掃描了 **50** 個 (含) 以上的連接埠，即假設為 TCP 連接埠	中等級適用相同規則。

掃描。 偵測到此現象時，即**記錄**攻擊者的 IP，但**不要新增**規則來封鎖攻擊。	掃描。 偵測到此現象時，即**記錄**攻擊者的 IP，並**新增**規則以封鎖攻擊。	

連接埠

只要在連結上按一下滑鼠就會顯示對話方塊，您可以在其中輸入掃描過多少個連接埠之後，會認定為 TCP 連接埠掃描。

連接埠掃描時間間隔

只要在此連結上按一下滑鼠就會顯示對話方塊，您可以在其中輸入在認定為 TCP 連接埠掃描活動之前，特定數量的連接埠掃描活動的時間間隔。

報告檔

只要在連結上按一下滑鼠，就可選擇記錄或是不記錄攻擊者的 IP 位址。

規則

只要在連結上按一下滑鼠，就可選擇新增或是不新增規則以封鎖 TCP 連接埠掃描攻擊。

UDP 連接埠掃描

有了這項規則，您就可以定義何時 FireWall 會認定為 UDP 連接埠掃描，以及在這種情況下需要採取的行動為何。此規則可預防所謂的 UDP 連接埠掃描攻擊，這種攻擊會偵測電腦上開放的 UDP 連接埠。此類攻擊會搜尋電腦上的弱點，並且經常伴隨著更危險的攻擊類型。

預先定義的 **UDP** 連接埠掃描規則

設定：低	設定：中	設定：高
如果在 **5,000** 毫秒內，掃描了 **50** 個 (含) 以上的連接埠，即假設為 UDP 連接埠掃描。 偵測到此現象時，即**記錄**攻擊者的 IP，但**不要新增**規則來封鎖攻擊。	如果在 **5,000** 毫秒內，掃描了 **50** 個 (含) 以上的連接埠，即假設為 UDP 連接埠掃描。 偵測到此現象時，即**記錄**攻擊者的 IP，並**新增**規則以封鎖攻擊。	中等級適用相同規則。

連接埠

只要在連結上按一下滑鼠就會顯示對話方塊，您可以在其中輸入掃描過多少個連接埠之後，會認定為 UDP 連接埠掃描。

連接埠掃描時間間隔

只要在此連結上按一下滑鼠就會顯示對話方塊，您可以在其中輸入在認定為 UDP 連接埠掃描活動之前，特定數量的連接埠掃描活動的時間間隔。

報告檔

只要在連結上按一下滑鼠，就可選擇記錄或是不記錄攻擊者的 IP 位址。

規則

只要在連結上按一下滑鼠，就可選擇新增或是不新增規則以封鎖 UDP 連接埠掃描攻擊。

13.4.1.1. 傳入規則

傳入規則可定義爲使用 Avira FireWall 來控制傳入的資料流量。

> **注意**
> 封包經過篩選之後，就會連續套用對應的規則，因此規則順序就非常重要。只有當您很清楚自己的行爲有何後果時才變更規則順序。

預先定義的 TCP 資料流量資料監視器規則

設定：低	設定：中	設定：高
無任何遭到 Avira FireWall 封鎖的傳入資料流量。	– 允許在 135 上建立的 TCP 連線 如果本機連接埠在 **{135}** 範圍內且遠端連接埠在 **{0-65535}** 範圍內，則**允許**來自位址 **0.0.0.0** (遮罩爲 **0.0.0.0**) 的 TCP 封包。 適用**現有連線的封包**。 **當封包符合規則時，不要記錄**。 進階：捨棄具有下列位元組的封包 **<空白>**、遮罩爲 **<空白>**、於位移 **0**。 – 拒絕 135 上的 TCP 封包 如果本機連接埠在 **{135}** 範圍內且遠端連接埠在 **{0-65535}** 範圍內，則拒絕來自位址 **0.0.0.0** (遮罩爲 **0.0.0.0**) 的 **TCP** 封包。 適用**所有封包**。 **當封包符合規則時，不要記錄**。	– 已建立監視的 TCP 資料流量 如果本機連接埠在 **{0-65535}** 範圍內且遠端連接埠在 **{0-65535}** 範圍內，則**允許**來自位址 **0.0.0.0** (遮罩爲 **0.0.0.0**) 的 TCP 封包。 適用**現有連線的封包**。 **當封包符合規則時，不要記錄**。 進階：捨棄具有下列位元組的封包 **<空白>**、遮罩爲 **<空白>**、於位移 **0**。

	進階：捨棄具有下列位元組的封包 **<空白>** 、遮罩為 **<空白>** 、於位移 **0** 。 – 監視 TCP 健康資料流量 如果本機連接埠在 **{0-65535}** 範圍內且遠端連接埠在 **{0-65535}** 範圍內，則**允許**來自位址 **0.0.0.0** (遮罩為 **0.0.0.0**) 的 TCP 封包。 適用**連線初始化和現有連線封包。** **當封包符合規則時，不要記錄**。 進階：捨棄具有下列位元組的封包 **<空白>**、遮罩為 **<空白>**、於位移 **0** 。 – 拒絕所有 TCP 封包 如果本機連接埠在 **{0-65535}** 範圍內且遠端連接埠在 **{0-65535}** 範圍內，則拒絕來自位址 **0.0.0.0** (遮罩為 **0.0.0.0**) 的 **TCP 封包**。 適用**所有封包**。 **當封包符合規則時，不要記錄**。 進階：捨棄具有下列位元組的封包 **<空白>**、遮罩為 **<空白>**、	

	於位移 **0**。	

<u>接受/拒絕 TCP 封包</u>

只要在連結上按一下滑鼠，就可選擇允許或是拒絕特別定義的傳入 TCP 封包。

<u>IP 位址</u>

只要在連結上按一下滑鼠，就會立即開啓對話方塊供您輸入所需的 IP 位址。

<u>IP 遮罩</u>

只要在此連結上按一下滑鼠，就會立即開啓對話方塊供您輸入所需的 IP 遮罩。

<u>本機連接埠</u>

只要在此連結上按一下滑鼠，就會立即顯示對話方塊供您定義本機連接埠編號或是完整的連接埠範圍。

<u>遠端連接埠</u>

只要在此連結上按一下滑鼠，就會立即顯示對話方塊供您定義遠端連接埠編號或是完整的連接埠範圍。

<u>套用方式</u>

只要在此連結上按一下滑鼠，就可選擇套用連線初始化與現有連線封包的規則，或是僅套用現有連線封包或所有封包的規則。

<u>報告檔</u>

只要在連結上按一下滑鼠，就可決定在封包符合規則時，是否寫入報告檔。

進階功能允許進行內容篩選設定。例如，當封包在特定位移包含某些特定資料時，就可以拒絕這些封包。如果您不想使用這個選項，請勿選取檔案，或是選擇空白檔案。

<u>已篩選內容：資料</u>

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您選取內含特定緩衝區的檔案。

<u>已篩選內容：遮罩</u>

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您選取特定遮罩。

<u>已篩選內容：位移</u>

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您定義篩選的內容位移。此位移是從 TCP 標頭結尾開始計算。

預先定義的 UDP 資料流量監視器規則

設定：低	設定：中	設定：高
-	– 監視 UDP 已接受的資料流量 如果本機連接埠在 **{0- 65535}** 範圍內且遠端連接埠在 **{0-65535}** 範圍內，則允許	已建立監視的 UDP 流量 如果本機連接埠在 **{0-65535}** 範圍內且遠端連接埠在 **{53, 67, 68, 123}** 範圍內，則允許來自位址 **0.0.0.0** (遮罩

	來自位址 **0.0.0.0** (遮罩爲 **0.0.0.0**) 的 UDP 封包。 套用規則至**開放的連接埠**。 **當封包符合規則時，不要記錄**。 進階：捨棄具有下列位元組的封包 **<空白>**、遮罩爲 **<空白>**、於位移 **0**。 – 拒絕所有 UDP 封包 如果本機連接埠在 **{0-65535}** 範圍內且遠端連接埠在 **{0-65535}** 範圍內，則拒絕來自位址 **0.0.0.0** (遮罩爲 **0.0.0.0**) 的 **UDP** 封包。 適用**所有連接埠**。 **當封包符合規則時，不要記錄**。 進階：捨棄具有下列位元組的封包 **<空白>**、遮罩爲 **<空白>**、於位移 **0**。	爲 **0.0.0.0**) 的 **UDP 封包**。 套用規則至**開放的連接埠**。 **當封包符合規則時，不要記錄**。 進階：捨棄具有下列位元組的封包 **<空白>**、遮罩爲 **<空白>**、於位移 **0**。

接受/拒絕 UDP 封包

只要在連結上按一下滑鼠，就可選擇允許或是拒絕特別定義的傳入 UDP 封包。

IP 位址

只要在連結上按一下滑鼠，就會立即開啓對話方塊供您輸入所需的 IP 位址。

IP 遮罩

只要在此連結上按一下滑鼠，就會立即開啓對話方塊供您輸入所需的 IP 遮罩。

本機連接埠

只要在此連結上按一下滑鼠，就會立即顯示對話方塊供您定義本機連接埠編號或是完整的連接埠範圍。

遠端連接埠

只要在此連結上按一下滑鼠，就會立即顯示對話方塊供您定義遠端連接埠編號或是完整的連接埠範圍。

<u>套用方式</u>

只要在此連結上按一下滑鼠，就可選擇將此規則套用至所有連接埠，或僅套用至所有開放的連接埠。

<u>報告檔</u>

只要在連結上按一下滑鼠，就可決定在封包符合規則時，是否寫入報告檔。

進階功能允許進行內容篩選設定。例如，當封包在特定位移包含某些特定資料時，就可以拒絕這些封包。如果您不想使用這個選項，請勿選取檔案，或是選擇空白檔案。

<u>已篩選內容：資料</u>

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您選取內含特定緩衝區的檔案。

<u>已篩選內容：遮罩</u>

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您選取特定遮罩。

<u>已篩選內容：位移</u>

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您定義篩選的內容位移。此位移是從 UDP 標頭結尾開始計算。

預先定義的 ICMP 資料流量監視器規則

設定：低	設定：中	設定：高
-	– 不要根據 IP 位址捨棄 ICMP **允許**來自位址 **0.0.0.0** (遮罩為 **0.0.0.0**) 的 ICMP 封包。 **當封包符合規則時，不要記錄。** 進階：捨棄具有下列位元組的封包 **<空白>**、遮罩為 **<空白>**、於位移 **0**。	中等級適用相同規則。

<u>接受/拒絕 **ICMP** 封包</u>

只要在連結上按一下滑鼠，就可選擇允許或是拒絕特別定義的傳入 ICMP 封包。

<u>**IP** 位址</u>

只要在連結上按一下滑鼠，就會立即開啓對話方塊供您輸入所需的 IP 位址。

<u>**IP** 遮罩</u>

只要在此連結上按一下滑鼠，就會立即開啓對話方塊供您輸入所需的 IP 遮罩。

<u>報告檔</u>

只要在連結上按一下滑鼠，就可決定在封包符合規則時，是否寫入報告檔。

進階功能允許進行內容篩選設定。例如，當封包在特定位移包含某些特定資料時，就可以拒絕這些封包。如果您不想使用這個選項，請勿選取檔案，或是選擇空白檔案。

已篩選內容：資料

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您選取內含特定緩衝區的檔案。

已篩選內容：遮罩

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您選取特定遮罩。

已篩選內容：位移

只要在連結上按一下滑鼠，就會立即顯示對話方塊供您定義篩選的內容位移。此位移是從 ICMP 標頭結尾開始計算。

預先定義的 IP 封包規則

設定：低	設定：中	設定：高
-	-	拒絕所有 IP 封包 拒絕來自位址 **0.0.0.0** (遮罩為 **0.0.0.0**) 的 **IP 封包**。 **當封包符合規則時，不要記錄**。

接受/拒絕 IP 封包

只要在連結上按一下滑鼠，就可決定是否要接受或拒絕特別定義的 IP 封包。

IP 位址

只要在連結上按一下滑鼠，就會立即開啟對話方塊供您輸入所需的 IP 位址。

IP 遮罩

只要在此連結上按一下滑鼠，就會立即開啟對話方塊供您輸入所需的 IP 遮罩。

報告檔

只要在連結上按一下滑鼠，就可決定在封包符合規則時，是否寫入報告檔。

依據 IP 通訊協定來監視 IP 封包時可用的規則

IP 封包

只要在連結上按一下滑鼠，就可決定是否要接受或拒絕特別定義的 IP 封包。

IP 位址

只要在連結上按一下滑鼠，就會立即開啟對話方塊供您輸入所需的 IP 位址。

IP 遮罩

只要在此連結上按一下滑鼠，就會立即開啟對話方塊供您輸入所需的 IP 遮罩。

通訊協定

只要在此連結上按一下滑鼠，就會立即開啟對話方塊供您輸入所需的 IP 通訊協定。

報告檔

只要在連結上按一下滑鼠，就可決定在封包符合規則時，是否寫入報告檔。

13.4.1.2. 傳出規則

傳出規則可定義爲使用 Avira FireWall 來控制傳出的資料流量。您可以爲下列其中一項通訊協定定義傳出的規則：IP、ICMP、UDP 與 TCP。

注意
封包經過篩選之後，就會連續套用對應的規則，因此規則順序就非常重要。只有當您很清楚自己的行爲有何後果時才變更規則順序。

按鈕

按鈕	**Description**
新增	允許您建立新的規則。如果您按下此按鈕，就會開啓 [新增規則] "對話方塊"。您可以在此對話方塊中選取新規則。
移除	移除選取的規則。
規則下移	將選取的規則下移一行，也就是降低規則的優先順序。
規則上移	將選取的規則上移一行，也就是提高規則的優先順序。
重新命名	允許您爲選取的規則賦予另一個名稱。

注意
您可以爲電腦上個別介面卡或所有介面卡新增規則。若要爲所有介面卡新增介面卡規則，從顯示的介面卡階層選取 **[電腦]**，然後按一下 **[新增]** 按鈕。

注意
若要變更規則位置，您還可以使用滑鼠將規則拖曳到所需的位置。

13.4.2 應用程式規則

使用者的應用程式規則

此清單包含系統中的所有使用者。如果您是以系統管理員身分登入，可以選取您要對其套用規則的使用者。如果您不是具有權限的使用者，則只能看到目前登入的使用者。

應用程式清單

此表顯示已定義規則的應用程式清單。應用程式清單包含了電腦上安裝 Avira FireWall 之後，曾經執行過而且已儲存規則的每個應用程式。

一般檢視

	Description
應用程式	應用程式名稱。
模式	顯示選取的應用程式規則模式 ：在**已篩選**模式中，會在應用程式規則執行之後檢查並執行介面卡規則。在*具有權限*模式中，會忽略介面卡規則。按一下連結，切換至不同的模式。
動作	顯示當應用程式正在使用網路時，Avira FireWall 將自動採取的行動 (不管網路使用類型為何)。使用滑鼠按一下連結時，可以切換為其他動作類型。動作類型分為**詢問**、**允許**或**拒絕**。**詢問**是預設動作。

<u>延伸組態</u>

如果應用程式的網路存取活動需要使用個別規則，則您可以依據封包篩選器並比照先前建立介面卡規則的方式來建立應用程式規則。若要將應用程式規則變更為延伸組態，請先啓用專家模式。接著在 FireWall::設定區段中變更應用程式規則設定：啓用 **[延伸的設定]** 選項並按一下 **[接受]** 或 **[確定]**，儲存相關設定。在防火牆組態中，選取 **[FireWall::應用程式規則]** 區段：在應用程式規則清單中會顯示具有 *[篩選]* 標題和 *[簡易]* 項目的額外欄位。您現在有額外的 **[篩選:** *進階 - 動作: 規則]* *選項，可讓您選取延伸組態。*

	Description
應用程式	應用程式名稱。
模式	顯示選取的應用程式規則模式 ：在**已篩選**模式中，會在應用程式規則執行之後檢查並執行介面卡規則。在*具有權限*模式中，會忽略介面卡規則。按一下連結，切換至不同的模式。
動作	顯示當應用程式正在使用網路時，Avira FireWall 將自動採取的行動 (不管網路使用類型為何)。 如果您選擇 *[篩選 - 簡易]*，可以按一下連結選取另一個動作類型。其中的值分為**詢問**、**允許**、**拒絕**或*延伸*。 如果您選擇 *[篩選 - 進階]*，則會顯示 *[規則]* 動作類型。**[規則]** 連結會開啓 **[應用程式規則]** 視窗，您可以在此輸入應用程式的特定規則。
篩選	顯示篩選類型。您可以按一下連結選取另一個篩選類型。 *簡易*：如果是簡易篩選，則會對軟體應用程式執行的所有網路活動進行指定的動作。 *進階*：如果是這種篩選類型，則會套用已加入延伸組態的規則。

如果您想要建立應用程式特定的規則，請選取 [篩選] 底下的 [進階] 項目。*[規則]* 項目隨即顯示在 **[動作]** 欄中。按一下 **[規則]** 即可開啓用來建立特定應用程式規則的視窗。

<u>延伸組態中的指定應用程式規則</u>

指定的應用程式規則可讓您針對應用程式允許或拒絕指定的資料流量，或是允許或拒絕被動聆聽個別連接埠。以下為可用的選項：

允許或拒絕植入程式碼

「植入程式碼」這項技巧可將程式碼引入另一個處理序的位址空間以執行相關動作，進而強制此處理序載入動態連結程式庫 (DLL)。惡意程式碼特別喜歡利用植入程式碼方式，以其他程式爲掩護來執行程式碼。如此一來，便可隱藏網際網路存取活動，不讓 FireWall 發現。預設模式會針對所有簽署的應用程式啓用植入程式碼功能。

允許或拒絕被動聆聽連接埠上的應用程式

允許或拒絕資料流量

允許或拒絕傳入與/或傳出的 IP 封包

允許或拒絕傳入與/或傳出的 TCP 封包

允許或拒絕傳入與/或傳出的 UDP 封包

您可以針對每一個應用程式，建立想要的應用程式規則，而且數量不限。 應用程式規則執行順序如下所示 (相關資訊請參閱)。

注意
如果您變更應用程式規則的 *[進階]* 篩選，已在延伸組態中的現有應用程式規則只是停用，並不會永久刪除。 如果您再次選取 [進階] 篩選，現有應用程式規則會重新啓用，並顯示在應用程式規則的延伸組態視窗中。

應用程式詳細資料

在此方塊中，您可以檢視應用程式清單方塊中選取的應用程式詳細資料。

	Description
名稱	應用程式名稱。
路徑	可執行檔的完整路徑。

按鈕

按鈕	**Description**
新增應用程式	允許您建立新的應用程式規則。如果您按下此按鈕，就會開啓對話方塊。您可在此選取所需的應用程式，以建立新規則。
移除規則	移除選取的應用程式規則。
重新載入	重新載入應用程式清單，並同時捨棄剛對應用程式規則進行的變更。

13.4.3 信任的供應商

[信任的供應商] 底下會顯示一份信任的軟體生產商清單。您可以透過 *[網路事件]* 快顯視窗裡的 *[一律信任此供應商]* 選項，從清單中新增或移除製造商。您可以啓用 **[自動允許受信任供應商的應用程式]** 選項，預設允許由清單中的供應商所簽署的應用程式網路存取行爲。

使用者的受信任供應商

此清單包含系統中的所有使用者。如果您是以系統管理員身分登入，可以選取要檢視或更新信任的供應商清單的使用者。如果您不是具有權限的使用者，則只能看到目前登入的使用者。

自動允許受信任供應商建立的應用程式

此選項一經啓用，會自動允許內含已知及受信任供應商簽章的應用程式存取網路。此選項會啓用爲預設值。

供應商

此清單列出歸類爲受信任的所有供應商。

按鈕

按鈕	**Description**
移除	反白的項目會從受信任的供應商清單中移除。若要從清單中永久移除選取的供應商，在組態視窗裡按一下 **[接受]** 或 **[確定]**。
重新載入	已回復所做的變更。已載入上次儲存的清單。

注意
如果您從清單中移除供應商，並選取 **[套用]**，則會從清單中永久移除供應商。使用 *[重新載入]* 無法回復變更。不過，您可以透過 *[網路事件]* 快顯視窗裡的 *[一律信任此供應商]* 選項，再次將供應商新增至受信任的供應商清單中。

注意
FireWall 會在將其他項目加入受信任的供應商清單之前，先處理好應用程式規則的優先順序：如果您已經建立應用程式規則，且應用程式供應商已列在受信任的供應商清單中，將會執行應用程式規則。

13.4.4 設定

進階選項

啓用 **FireWall**

此選項一經啓用，就會啓用 Avira FireWall，保護您的電腦免於源自網際網路和其他網路的風險。

<u>啓動時停止 **Windows** 防火牆</u>

此選項一經啓用，一旦電腦重新開機，就會停用 Windows 防火牆。此選項會啓用爲預設值。

<u>**Windows** 主機檔案尚未鎖定/已鎖定</u>

如果此選項設爲「已鎖定」，則 Windows 主機檔案會加上寫入保護。以後無法再進行操作。例如，惡意程式碼將無法把您重新導向至有害的網站。此選項狀態預設爲「未鎖定」。

自動規則逾時

<u>永遠封鎖</u>

此選項一經啓用，舉例來說，會保留在連接埠掃描期間自動建立的規則。

<u>在 **n** 秒後移除規則</u>

此選項一經啓用，舉例來說，在連接埠掃描期間自動建立的規則會在經過您定義的時間之後再次遭到移除。此選項會啓用爲預設值。

通知

通知項目可定義您希望從 FireWall 收到桌面通知的相關事件。

<u>連接埠掃描</u>

此選項一經啓用，只要 FireWall 偵測到連接埠掃描，您就會收到桌面通知。

<u>洪水攻擊</u>

此選項一經啓用，只要 FireWall 偵測到洪水攻擊，您就會收到桌面通知。

<u>封鎖的應用程式</u>

此選項一經啓用，只要 FireWall 拒絕活動 (例如封鎖了某個應用程式的網路活動)，您就會收到桌面通知。

<u>封鎖的 **IP**</u>

此選項一經啓用，只要 FireWall 拒絕活動 (例如封鎖了來自某個 IP 位址的資料流量)，您就會收到桌面通知。

應用程式規則

您可在 FireWall::應用程式規則區段中，使用應用程式規則選項來設定其組態選項。

<u>進階選項</u>

此選項一經啓用，就可以個別規定應用程式的網路存取行爲。

<u>基本設定</u>

此選項一經啓用，不同的應用程式網路存取行爲只能設定一項動作。

13.4.5 快顯設定

快顯設定

<u>檢查處理序啓動堆疊</u>

此選項一經啓用，便可更精準地控制處理序堆疊偵測作業。FireWall 會假定堆疊中只要有任何一個處理序實際上透過所屬的子處理序來存取網路的處理序，就不值得信賴。因此，處理序堆疊會針對每個不值得信賴的處理序開啓個別的快顯視窗。預設會停用此選項。

<u>允許每個處理序有多個快顯</u>

此選項一經啓用，每次應用程式進行網路連線時，就會觸發快顯視窗。或者，您只會在第一次連線嘗試時才會收到通知。預設會停用此選項。

<u>在遊戲模式時，自動隱藏快顯通知</u>

若此選項已經啓用，當您於電腦系統全螢幕模式下執行應用程式，會自動啓動 Avira FireWall 遊戲模式。在遊戲模式中，會套用所有定義的介面卡與應用程式規則。系統允許尚未定義 "*[允許]*" 或 "*[拒絕]*" 動作規則的應用程式，可暫時存取網路，這樣就不會出現詢問有關網路事件問題的快顯視窗。

記住對此應用程式採取的動作

<u>一律啓用</u>

一旦啓用此選項，會啓用 [網路事件] 對話方塊裡預設的 [記住對此應用程式採取的動作]""""。此選項會啓用為預設值。

<u>一律停用</u>

一旦啓用此選項，會停用 [網路事件] 對話方塊裡預設的 [記住對此應用程式採取的動作]""""。

<u>僅對已簽署的應用程式啓用</u>

一旦啓用此選項，簽署的應用程式會在網路存取期間自動啓用 [網路事件] 對話方塊裡預設的 [記住對此應用程式採取的動作] 選項。""""製造商包括：Microsoft、Mozilla、Opera、Yahoo、Google、Hewlet Packard、Sun、Skype、Adobe、Lexmark、Creative Labs、ATI、nVidia。

<u>記住上次使用的狀態</u>

一旦啓用此選項，[網路事件] 對話方塊中的 [記住對此應用程式採取的動作] 選項啓用狀態，會比照上次的網路事件。""""如果 [網路事件] 對話方塊裡的 [記住對此應用程式採取的動作] 選項已啓用，則後續的網路事件便會啓用此選項。""如果已針對上次網路事件停用 [記住對此應用程式採取的動作] 選項，則後續的網路事件也會停用此選項。""

顯示詳細資料

在此組態選項群組中，您可以設定 **[網路事件]** 視窗中中的詳細資訊顯示方式。

<u>應要求顯示詳細資料</u>

此選項一經啓用，詳細資訊只會應要求顯示在 [網路事件] 視窗。例如，您可以按一下 [網路事件] 視窗中的 [顯示詳細資料] 按鈕，顯示詳細資訊。""""""

<u>一律顯示詳細資料</u>

此選項一經啓用，一律在 "*[網路事件]*" 視窗中顯示詳細的資訊。

<u>記住上次使用的狀態</u>

此選項一經啓用，會使用先前管理網路事件的方式來管理詳細資訊的顯示方式。如果在上次網路事件期間曾經檢視或存取詳細資訊，則後續的網路事件也會顯示詳細資訊。如果在上次網路事件期間曾經隱藏而不顯示詳細資訊，則後續網路事件便不會顯示詳細資訊。

允許具特殊權限者

在此組態選項群組中，您可以定義 **[網路事件]** 視窗中的 *[允許具特殊權限者]* 選項狀態。

<u>一律啓用</u>

此選項一經啓用，"*[允許具特殊權限者]*" 選項便會啓用成爲 "*[網路事件]*" 視窗中的預設值。

<u>一律停用</u>

此選項一經啓用，"*[允許具特殊權限者]*" 選項便會停用並成爲 "*[網路事件]*" 視窗中的預設值。

<u>記住上次使用的狀態</u>

此選項一經啓用，"*[允許具特殊權限者]*" 選項的狀態便會比照 "*[網路事件]*" 視窗中前一個網路事件的處理方式：如果在上次網路事件的執行期間，啓用了 "*[允許具特殊權限者]*"，後續網路事件便會預設啓用此選項。如果在上次網路事件的執行期間，停用了 "*[允許具特殊權限者]*" 選項，後續網路事件便會依此預設而停用此選項。

13.5 WebGuard

[組態] 的 [WebGuard] 區段負責 WebGuard 的組態。

13.5.1 掃描

WebGuard 可針對各種透過網際網路載入網頁瀏覽器的網頁，防範藉此抵達您電腦的病毒或惡意程式碼。*[掃描]* 標題可用來設定 WebGuard 元件的行爲。

掃描

<u>啓用 **WebGuard**</u>

此選項一經啓用，會掃描透過網際網路瀏覽器所要求的網頁，查看其中是否有病毒與惡意程式碼。WebGuard 會監視透過 HTTP 通訊協定，連接埠 80、8080、3128 從網際網路傳輸的資料。如果偵測到任何受影響的網頁，就會封鎖網頁不讓其載入。此選項一經停用，WebGuard 服務仍是開啓狀態，但是會停用病毒與惡意程式碼的掃描。

注意
若要使用家長監護功能，您一定要啓用 WebGuard。

偷渡式攻擊保護

偷渡式攻擊保護可讓您設定封鎖 I-Frame (亦稱爲內置框架)。I-Frame 是 HTML 元件，亦即區隔網頁區域的網際網路頁面元素。I-Frame 可用來載入不同的網頁內容 (通常是其他的 URL) 並在瀏覽器的子視窗中將其顯示爲獨立的文件。I-Frame 大部分用來提供橫幅廣告服務。在某些情況下，I-Frames 會被用來隱藏惡意程式碼。在這些情況下，瀏覽器幾乎是看不到 I-Frame 區域的。*[封鎖可疑的 I-frames]* 選項可讓您檢查與封鎖載入的 I-Frame。

封鎖可疑的 I-frames

此選項一經啓用，會依據特定準則掃描您所要求網頁上的 I-Frame。如果要求的網頁上有可疑的 I-Frame，會將其封鎖。I-Frame 視窗中顯示錯誤訊息。

預設値

此選項一經啓用，會封鎖內含可疑內容的 I-Frame。

進階

此選項一經啓用，會封鎖內含可疑內容且使用方式可疑的 I-Frame。如果 I-Frame 體積很小以致於在瀏覽器上看不到或幾乎看不到，或者 I-Frame 放在網頁上不尋常的位置時，這類的 I-Frame 用途就可視爲可疑。

13.5.1.1. 偵測有所發現時採取的動作

偵測有所發現時採取的動作

您可以定義當偵測到病毒或有害程式時，WebGuard 要執行的動作。

互動式

此選項一經啓用，一旦在指定掃描期間偵測到病毒或有害程式時會顯示對話方塊，供您選擇對受影響檔案的處置方式。此選項會啓用爲預設値。

如需詳細資訊，按一下此處。

顯示進度列

此選項一經啓用，當網站內容下載時間超過 20 秒的逾時規定時，桌面上會出現包含下載進度列的通知。此桌面通知係針對下載網站內含較大量資料時所特別設計：如果您使用 WebGuard 來瀏覽，網站內容不會以增量方式下載到網際網路瀏覽器中，因爲這些內容在透過網際網路瀏覽器顯示之前，會先掃描是否有病毒與惡意程式碼。預設會停用此選項。

自動

此選項一經啓用，偵測到病毒時將不會出現任何對話方塊。WebGuard 會根據您在這個區段中預先定義爲主要和次要動作的設定來反應。

主要動作

主要動作是 WebGuard 發現病毒或有害程式時優先執行的動作。

拒絕存取

網路伺服器要求的網站與/或傳輸的任何資料或檔案，都不會傳送到您的網頁瀏覽器。網頁瀏覽器上會顯示一則錯誤訊息，通知您已經拒絕存取。WebGuard 會在報告功能啓用時，將偵測結果記錄到報告檔案。

隔離

偵測到病毒或惡意程式碼時，網路伺服器要求的網站與/或傳輸的任何資料或檔案，都會移至隔離區。如果受影響的檔案具有任何參考價值，可以從隔離區管理員復原，或在必要時將其傳送至 Avira 惡意程式碼研究中心。

略過

WebGuard 會將網路伺服器要求的網站與/或傳輸的資料與檔案，傳送到您的網頁瀏覽器。允許存取檔案並忽略檔案。

警告
工作站上受影響的檔案仍會繼續運作！此做法可能會對工作站造成嚴重的傷害！

13.5.1.2. 鎖定的要求

您可以在 **[鎖定的要求]** 中，指定 WebGuard 要封鎖的檔案類型與 MIME 類型 (傳輸資料的內容類型)。網路篩選器可讓您封鎖網路釣魚和惡意程式碼 URL。WebGuard 可預防資料從網際網路傳輸到您的電腦系統上。

WebGuard 要封鎖的檔案類型/MIME 類型 (使用者定義)

清單中的所有檔案類型與 MIME 類型 (傳輸資料的內容類型) 會遭到 WebGuard 封鎖。

輸入方塊

請在此方塊中，輸入您希望 WebGuard 封鎖的 MIME 類型與檔案類型名稱。請針對檔案類型輸入副檔名，例如 **.htm**。針對 MIME 類型，請指出媒體類型與子類型 (適用的話)。兩個陳述式之間可以使用單斜線來分隔，例如 **video/mpeg** 或 **audio/x-wav**。

注意
不過，已經以網際網路暫存檔形式存放在電腦系統，並遭到 WebGuard 封鎖的檔案，可以由電腦的網際網路瀏覽器從網際網路下載到本機。網際網路暫存檔指的是由網際網路瀏覽器儲存在電腦上的檔案，可供您更快速地存取網站。

注意
如果您將封鎖的檔案與 MIME 類型清單輸入到排除的檔案與 MIME 類型清單 (於 WebGuard::掃描::例外底下)，則會略過此清單。

注意
輸入檔案類型與 MIME 類型時，無法使用任何萬用字元 (* 代表任何數量的字元，而 ? 則代表單一字元)。

MIME 類型：媒體類型範例：

– `text` = 代表文字檔案
– `image` = 代表圖形檔案
– `video` = 代表視訊檔案
– `audio` = 代表聲音檔案
– `application` = 代表與特定程式連結的檔案

例如：排除的檔案與 MIME 類型

– `application/octet-stream` = 應用程式/octet-stream MIME 類型檔案 (可執行檔 *.bin、*.exe、*.com、*dll、*.class) 都會遭到 WebGuard 封鎖。
– `application/olescript` = 應用程式/olescript MIME 檔案類型 (ActiveX 指令碼檔案 *.axs) 都會遭到 WebGuard 封鎖。

- `.exe` = 所有帶有副檔名 .exe (可執行檔) 的檔案都會遭到 WebGuard 封鎖。
- `.msi` = 所有帶有副檔名 .msi 的檔案 (Windows Installer 檔案) 都會遭到 WebGuard 封鎖。

新增

此按鈕可讓您從輸入欄位中，將 MIME 與檔案類型複製到顯示視窗。

刪除

此按鈕會從清單刪除選取的項目。如果沒有選取任何項目，此按鈕將無作用。

網路篩選器

網路篩選器以內部資料庫爲基礎，會每日更新並依據內容來分類 URL。

啓用網路篩選器

選項一經啓用，符合網路篩選器清單中選取類別的所有 URL 都會遭到封鎖。

網路篩選器清單

在網路篩選器清單中，您可以選取要讓 WebGuard 封鎖其 URL 的內容類別。

注意
網路篩選器會略過排除的 URL 清單中的項目 (於 WebGuard::掃描::例外底下)。

注意
垃圾郵件 URL 指的是透過垃圾電子郵件傳送的 URL。「詐騙」類別涵蓋帶有“「訂閱到期」”與其他由供應商隱藏成本的服務項目等特徵的相關網頁。

13.5.1.3. 例外

這些選項可讓您依據 URL (網際網路位址) 的 MIME 類型 (傳輸資料的內容類型) 與檔案類型，設定 WebGuard 的掃描例外。WebGuard 會略過指定的 MIME 類型與 URL，亦即不會針對傳輸到電腦系統的資料掃描其中是否有病毒與惡意程式碼。

WebGuard 略過的 MIME 類型

您可以在此欄位中，選取要讓 WebGuard 在掃描期間略過的 MIME 類型 (傳輸資料的內容類型)。

WebGuard 略過的檔案類型/MIME 類型 (使用者定義)

WebGuard 會在掃描期間略過清單中的所有 MIME 類型 (傳輸資料的內容類型)。

輸入方塊

您可以在此方塊中，輸入要讓 WebGuard 在掃描期間略過的 MIME 類型與檔案類型名稱。請針對檔案類型輸入副檔名，例如 **.htm**。針對 MIME 類型，請指出媒體類型與子類型 (適用的話)。兩個陳述式之間可以使用單斜線來分隔，例如 **video/mpeg** 或 **audio/x-wav**。

注意
輸入檔案類型與 MIME 類型時，無法使用任何萬用字元 (* 代表任何數量的字元，而 ? 則代表單一字元)。

警告
排除清單上的所有檔案類型與內容類型都會下載到網際網路瀏覽器，不需要再經過封鎖存取 (在 WebGuard::掃描::封鎖存取中封鎖的檔案與 MIME 類型清單) 或 WebGuard 的掃描：針對排除清單上的所有項目，會略過要封鎖的檔案與 MIME 類型清單上的項目。不會執行病毒與惡意程式碼掃描。

MIME 類型：媒體類型範例：

– `text` = 代表文字檔案
– `image` = 代表圖形檔案
– `video` = 代表視訊檔案
– `audio` = 代表聲音檔案
– `application` = 代表與特定程式連結的檔案

例如：排除的檔案與 MIME 類型

– `audio/` = 代表要從 WebGuard 掃描中排除的所有音訊媒體類型檔案
– `video/quicktime` = 代表要從 WebGuard 掃描中排除的所有 Quicktime 子類型視訊檔案 (*.qt、*.mov)
– `.pdf` = 代表要從 WebGuard 掃描中排除的所有 Adobe PDF 檔案。

新增

此按鈕可讓您從輸入欄位中，將 MIME 與檔案類型複製到顯示視窗。

刪除

此按鈕會從清單刪除選取的項目。如果沒有選取任何項目，此按鈕將無作用。

WebGuard 略過的 URL

此清單中的所有 URL 會從 WebGuard 掃描中排除。

輸入方塊

您可以在此方塊中輸入要排除不進行 WebGuard 掃描的 URL (網際網路位址)，例如 **www.domainname.com**。您可以使用前導或後續句點來指出網域層級，藉此指定 URL 的各部分：.domainname.com 代表網域的所有網頁與所有子網域。使用後續句點來指定任何頂層網域 (.com 或 .net) 的網站：domainname.。如果您不使用前導或結尾句點來指定字串，會將字串解譯為頂層網域，例如 **net** 可代表所有 NET 網域 (www.domain.net)。

注意
指定 URL 時，您也可以使用萬用字元 * 來代表任何數量的字元。您也可以使用前導或後續句點並結合萬用字元來指定網域層級：
.domainname.*
*.domainname.com
.*name*.com (有效的格式，但不建議採用)
不含句點的指定項目，例如 *name*，會解譯為頂層網域的一部分，因此不建議使用。

警告
排除 URL 清單上的所有網站都會下載到網際網路瀏覽器中，不會經由網路篩選器或 WebGuard 做進一步的掃描。至於排除 URL 清單中的所有項目，會略過網路篩選器中的項目 (請參閱 WebGuard::掃描::封鎖存取)。不會執行病毒與惡意程式碼掃描。因此，請僅讓信任的 URL 從 WebGuard 掃描中排除。

新增

此按鈕可讓您將輸入到輸入欄位中的 URL (網際網路位址)，複製到檢視器視窗。

刪除

此按鈕會從清單刪除選取的項目。如果沒有選取任何項目，此按鈕將無作用。

例如：略過的 URL

– `www.avira.com` -或- `www.avira.com/*`

= 所有內含 'www.avira.com' 網域的 URL 都會從 WebGuard 掃描中排除：www.avira.com/en/pages/index.php、www.avira.com/en/support/index.html、www.avira.com/en/download/index.html 等等。
內含 'www.avira.de' 網域的 URL 不會從 WebGuard 掃描中排除。

– `avira.com` -或- `*.avira.com`

= 所有內含 'avira.com' 之第二層與頂層網域的 URL 都會從 WebGuard 掃描中排除：此規定意指 '.avira.com' 的所有現有子網域：www.avira.com、forum.avira.com 等等。

– `avira.`-或- `*.avira.*`

= 所有內含 'avira' 之第二層網域的 URL 都會從 WebGuard 掃描中排除：此規定意指 '.avira' 的所有現有頂層網域或子網域：www.avira.com、www.avira.de、forum.avira.com 等等。

– `.*網域*.*`

所有內含 'domain' 字串之第二層網域的 URL 都會從 WebGuard 掃描中排除：www.domain.com、www.new-domain.de、www.sample-domain1.de 等等。

– `net` -或- `*.net`

= 所有內含 'net' 之頂層網域的 URL 都會從 WebGuard 掃描中排除：www.name1.net、www.name2.net 等等。

警告
盡可能準確地輸入要從 WebGuard 掃描中排除的 URL。請避免指定整個頂層網域或部分第二層網域，因爲這類全域排除設定可能會導致 WebGuard 掃描漏掉會散佈惡意程式碼與有害程式的網頁。建議您至少指定完整的第二層網域與頂層網域：domainname.com

13.5.1.4. 啓發式掃毒

此組態區段包含掃描引擎的啓發式掃毒設定。

AntiVir 產品內含威力非常強大的啓發式掃毒模組，可主動發現不明的惡意程式碼，亦即可在完成用來對抗破壞元素的特殊病毒簽章之前，並在病毒保護更新傳送之前先行制敵機先。病毒偵測作業牽涉到針對受影響的程式碼，深入分析並調查其中有無惡意程式碼的典型功能。如果掃描的程式碼表現出相關特徵，就會回報爲可疑。但這並不代表程式碼本身就是惡意程式碼。有時可能會出現誤判。使用者必須依據個人對於程式碼來源是否可信任的了解，決定如何處置受影響的程式碼。

巨集病毒啓發式掃毒

巨集病毒啓發式掃毒

您的 AntiVir 產品包含威力非常強大的病毒啓發式掃毒工具。此選項一經啓用，在修復期間，相關文件上的所有巨集都會被刪除，或者只是針對可疑的文件加以回報，亦即，您會收到警示。系統不只預設啓用此選項，也建議使用這個選項。

先進啓發式掃毒分析與偵測 (AHeAD)

啓用 **AHeAD**

您的 AntiVir 程式內含威力強大的 AntiVir AHeAD 啓發式掃毒技術，此技術可同時偵測不明 (新型態) 惡意程式碼。此選項一經啓用，您可以定義此啓發式掃毒技術的「積極」程度。""此選項會啓用爲預設值。

低偵測等級

此選項一經啓用，將可偵測到稍微不明的惡意程式碼，而在此情況下錯誤警示的機率並不高。

中偵測等級

如果您已選取使用此啓發式掃毒技術，這將會是預設選項。

高偵測等級

此選項一經啓用，將可偵測到極度不明的惡意程式碼，不過也更可能發生誤判。

13.5.2 報告

WebGuard 包含延伸的記錄功能，提供使用者或系統管理員有關偵測類型與方法的準確記錄。

報告功能

此群組可決定報告檔案內容。

關閉

此選項一經啓用，WebGuard 便不會建立記錄。
建議您只有在例外情況下才關閉記錄功能，例如當您對多個病毒或有害程式執行試用版軟體時。

預設值

此選項一經啓用，WebGuard 會將重要的資訊 (有關病毒偵測、警示與錯誤事項) 記錄到報告檔中，並忽略較不重要的資訊，讓報告更爲簡明易懂。此選項會啓用爲預設值。

進階

此選項一經啓用，WebGuard 會將較不重要的資訊同時包含在報告檔中。

完整

此選項一經啓用，WebGuard 會將所有可用資訊記錄到報告檔中，包括檔案大小、檔案類型、日期等等。

限制報告檔

將大小限制爲

此選項一經啓用，可將報告檔大小限定爲特定大小。可能的值如下：允許介於 1 到 100 MB 之間的值。當限制報告檔大小以節省系統資源時，允許使用約 50 KB 的額外空間。如果記錄檔大小超出指定大小 50 KB 以上，會先刪除舊的項目，直到達到指定大小減去 20%。

縮短報告前先備份

此選項一經啓用，縮短報告檔案前會先加以備份。

在報告檔中寫入組態

此選項一經啓用，會將即時掃描的組態記錄在報告檔中。

注意
如果您尚未指定任何報告檔限制，當此報告檔達到 100MB 時，舊項目會自動刪除。項目將遭到刪除，直到報告檔大小達到 80 MB。

13.6 家長監護

您的 AntiVir 程式的家長監護功能可篩選有害或是非法的網際網路內容以及限制網際網路使用的時間。家長監護功能是 WebGuard 元件的一部分。您可以將使用者角色指派給電腦使用者。使用者角色是可設定的，包含有下列準則的規則集：

– 禁止或允許的 URL (網際網路位址)
– 禁止的內容類別
– 網際網路使用持續時間以及必要時允許的週間日使用期限

當系統依據特定類別來封鎖網際網路內容時，會使用威力強大的 URL 篩選清單，以網際網路頁面內容爲基礎將內容分類爲不同的群組。URL 篩選清單每小時執行一次更新、調整和擴充。兒童、青少年與成人角色會以相關的禁止類別來加以預先設定。

網際網路使用記錄是以至少長達 5 分鐘的網際網路要求爲基準。

家長監護功能一經啓用，會依據使用者角色來檢查使用者在瀏覽網際網路時所要求的所有網頁。如果是禁止的網頁，會加以封鎖並在瀏覽器上顯示一則訊息。 如果已超過許可的使用期間或嘗試在許可的使用期間外使用，則會封鎖所要求的網站，並在瀏覽器上顯示一則訊息。

警告
請注意，若要使用家長監護功能，您必須啓用 WebGuard 服務。

警告
啓用家長監護功能時，請使用密碼來保護您的 AntiVir 程式組態。如果沒有使用密碼來保護組態，所有的電腦使用者都可以更改或停用家長監護設定。您可在 [一般]::[密碼] 底下啓用密碼保護。

如果您已經配置家長監護密碼，家長監護組態隨即隱藏，而 *[密碼保護]* 按鈕則會顯示。

密碼保護

若要啓用家長監護組態，請按 **"[密碼保護]"** 按鈕，並在 *"[輸入密碼]"* 視窗中輸入家長監護密碼。

啓用家長監護

此選項一經啓用，家長監護功能會依據指派給註冊使用者的角色，檢查使用者在瀏覽網際網路時所要求的所有網頁。如果指派的角色已將這些要求的網頁歸類爲禁止，便會加以封鎖。

注意
家長監護功能一經啓用，系統會針對先前設定家長監護時尚未指派角色的電腦*標準*使用者，指派*兒童*角色。您可以變更標準使用者的角色。
安裝後，會建立兒童、青少年和成人使用者角色。預先設定的角色已停用網際網路使用時間限制。

使用者選擇

使用者角色清單

此清單會顯示所有已指派角色的新增使用者。新增使用者時，程式預設會指派*兒童*角色。使用滑鼠按一下顯示的角色時，可以切換爲其他角色。

使用者

此清單包含系統中的所有使用者。

新增

您可以使用此按鈕，將選取的使用者新增至保護的使用者清單中。

刪除

此按鈕會從清單刪除選取的項目。

注意
無法刪除標準使用者。

角色

清單

此清單會顯示所有新增的角色。按兩下顯示的角色，可以開啓定義角色的對話方塊。

輸入方塊

您可以在此欄位中，輸入要新增至使用者角色的角色名稱。

變更

"[編輯]" 按鈕可用來設定選取的角色。這時會顯示對話方塊，供您針對角色定義禁止與允許的 URL，並依據類別定義選取的禁止網頁內容。

新增

藉由這個按鈕，您可以將輸入到輸入方塊中的角色新增至可用的角色清單中。

刪除

此按鈕會從清單刪除反白的角色。

注意
已經指派給使用者的角色無法刪除。

角色屬性

[編輯] 按鈕會帶您進入 *[角色屬性]* 對話方塊，供您針對禁止與允許的 URL 以及禁止的網頁內容定義使用者角色。以下為可用的選項：

– 禁止存取 URL
– 允許存取 URL
– 封鎖網頁內容：您可以針對要封鎖的網頁內容選取類別。
– 限制網際網路使用時間：您可以設定許可的使用期間 (每天、週、月)。 可啓用精確的週間日使用期限。

13.7 備份

[組態] 的 [更新] 區段負責 Avira 備份元件的組態。

13.7.1 設定

您可以在 **[設定]** 中，設定備份元件的行為。

設定

僅備份經過修改的檔案

此選項一經啓用，會建立增量備份：只有上次備份後修改的檔案會儲存到備份設定檔中。如果已停用此選項，系統會針對每個儲存的備份設定檔建立完整備份：所有檔案會儲存在備份設定檔中。系統不只預設啓用此選項，也建議使用這個選項，因為與完整資料備份相較之下，增量備份的建立速度較快，也較不耗用資源。

備份前先掃描有無病毒或有害的程式

此選項一經啓用，會在備份期間掃描儲存的檔案中是否有病毒與惡意程式碼。檔案只要受到感染，就不會儲存起來。系統不只預設啓用此選項，也建議使用這個選項。

13.7.2 例外

在各種例外情況下，您可以指定備份時要儲存與不儲存的檔案物件與檔案類型。

不要納入備份的檔案

本視窗中的清單包含備份中未儲存的檔案與路徑。

注意
清單中的項目結果總數不得超過 6000 個字元。

注意
此清單上的檔案已全部記錄在報告檔案中。

<u>輸入方塊</u>

在此方塊中輸入不要儲存的檔案物件名稱。預設會輸入已登入使用者的本機設定暫存目錄路徑。



此按鈕會開啟新的視窗，供您選取必要的檔案或路徑。
如果您擁有檔案的完整名稱與路徑，則可以從備份中隔離特定檔案。如果您已經輸入檔案名稱或路徑，就不會儲存具有此名稱的每個檔案 (無論檔案路徑或所屬磁碟機爲何)。

<u>新增</u>

藉由這個按鈕，您可以將輸入到輸入方塊中的檔案物件新增至顯示視窗。

<u>刪除</u>

此按鈕會從清單刪除選取的項目。如果沒有選取任何項目，此按鈕將無作用。

<u>重設清單</u>

此按鈕會還原預先定義的預設值。

<u>請注意下列各點：</u>

- 檔名只能包含萬用字元 * (任何數量的字元) 與 ? (單一字元)。
- 此清單將由上而下進行處理。
- 如果排除目錄，會一併自動排除所有子目錄。
- 也會排除個別副檔名 (內含萬用字元)。
- 爲了排除使用簡短 DOS 檔名 (8.3 DOS 名稱慣例) 存取的物件，還必須在清單中輸入相關的簡短檔名。

注意
內含萬用字元的檔名不可以反斜線來結束。

例如：

```
C:\Program Files\Application\applic*.exe\
```

此項目無效，且不會被視爲例外！

<u>例如：</u>

```
application.exe
\Program Files\
C:\*.*
C:\*
*.exe
*.xl?
*.*
C:\Program Files\Application\application.exe
C:\Program Files\Application\applic*.exe
C:\Program Files\Application\applic*
```

```
C:\Program Files\Application\applic?????.e*
C:\Program Files\
C:\Program Files
C:\Program Files\Application\*.mdb
```

副檔名清單

考慮所有副檔名

此選項一經啓用，將儲存備份設定檔中的所有檔案。

啓用略過副檔名的備份

此選項一經啓用，會儲存備份設定檔中的所有檔案 (已輸入排除的副檔名清單中的檔案則除外)。

副檔名

此按鈕會開啓對話方塊，顯示當啓用 [排除的副檔名] ""選項時，未在備份期間儲存的所有副檔名。系統會針對副檔名設定預設項目，不過您可以新增或刪除這些項目。

啓用納入副檔名清單的備份

此選項一經啓用，只會儲存其副檔名已經輸入至要考慮的副檔名清單中的檔案。

副檔名

此按鈕會開啓對話方塊，顯示當啓用 [包含的副檔名] 選項時，在備份期間儲存的所有副檔名。""系統會針對副檔名設定預設項目，不過您可以新增或刪除這些項目。

13.7.3 報告

備份元件包含完整的記錄功能。

報告功能

此群組可決定報告檔案內容。

關閉

此選項一經啓用，備份元件便無法建立記錄。請只有在例外情況下才關閉記錄功能。

預設值

此選項一經啓用，備份元件會將重要的資訊 (有關儲存、病毒偵測、警示與錯誤事項) 記錄到報告檔中，並忽略較不重要的資訊，讓報告更爲簡明易懂。此選項會啓用爲預設值。

進階

此選項一經啓用，備份元件會將較不重要的資訊包含在報告檔中。

完整

此選項一經啓用，備份元件會將備份處理序及病毒掃描的所有相關資訊都包含在報告檔中。

13.8 更新

您可以在 *[更新]* 區段中設定自動接收更新。 您可以指定各種更新間隔以及啓用或停用自動更新。

自動更新

啓用

此選項一經啓用，就會在指定的間隔執行啓用事件的自動更新。

每 **n** 天 **/** 小時 **/** 分鐘自動更新一次

在此方塊中，您可以指定執行自動更新的間隔。若要變更更新間隔，請反白方塊的其中一個時間選項，使用輸入方塊右方的箭號加以變更。

連線至網際網路時開始工作 (撥號連線)

此選項一經啓用，除了指定的更新間隔之外，只要建立網際網路連線，就會執行更新工作。

如果時間已過，重新執行工作

此選項一經啓用，就會執行過去在指定時間無法執行的更新工作，例如，因爲電腦關機而無法執行的工作。

13.8.1 開始更新產品

在 **[產品更新]** 底下，設定產品更新或可用產品更新通知的處理方式。

產品更新

下載並自動安裝產品更新

此選項一經啓用，一旦有可用的更新，更新程式元件就會立即下載產品更新並自動安裝。不管此設定爲何，您都可以獨立進行病毒定義檔與掃描引擎的更新。此選項條件如下：完整的更新組態與下載伺服器的開放式連線。

下載產品更新。如果需要重新啓動，請在系統重新啓動之後再安裝更新，否則請立即安裝更新。

此選項一經啓用，一旦有可用的新產品更新時，就會下載產品更新。如果不需要重新啓動，下載更新檔案後就會自動安裝這項更新。如果產品更新要求重新啓動電腦，下次使用者控制的系統重新開機時才會執行重新啓動，而不是在下載更新檔案後立即執行。其優點是，當使用者在電腦工作時不會執行重新啓動。不管此設定爲何，您都可以獨立進行病毒定義檔與掃描引擎的更新。此選項條件如下：完整的更新組態與下載伺服器的開放式連線。

可取得產品更新時，通知使用者

此選項一經啓用，一旦有可用的新產品更新時，您就會收到電子郵件通知。不管此設定爲何，您都可以獨立進行病毒定義檔與掃描引擎的更新。此選項條件如下：完整的更新組態與下載伺服器的開放式連線。您可以透過桌面快顯視窗與更新程式的警示 (於控制中心的 [概觀::事件] 底下)，接收通知。

在以下天數後，再通知一次

如果未在初始通知後安裝產品更新，請在此方塊中輸入在經過幾天後再次通知您可取得產品更新。

[不要下載產品更新]

此選項一經啓用，便無法執行自動產品更新或是由更新程式發出可用產品更新通知。不管此設定爲何，您都可以獨立進行病毒定義檔與搜尋引擎的更新。

重要
不管產品更新設定爲何，您都可以在每次更新處理序期間執行病毒定義檔與搜尋引擎的更新 (請參閱 更新一章裡的說明)。

注意
如果您已經啓用自動產品更新選項，可以在重新啓動設定底下設定其他重新啓動通知和取消選項。

13.8.2 重新啓動設定

由 AntiVir 程式執行產品更新時，您可能必須重新啓動電腦系統。如果您已經選取一般::更新::產品更新底下的自動產品更新，可以在 **[重新啓動設定]** 底下選擇不同的重新啓動通知和重新啓動取消選項。

注意
請注意，重新啓動設定可讓您在組態的一般::更新::產品更新底下，有關執行產品更新需要電腦重新啓動的兩個選項擇其一。

有可用更新時自動執行產品更新與必要的電腦重新啓動：當使用者在電腦工作，同時會執行更新和重新啓動。 如果您已啓用此選項，最好選取有取消選項或提醒功能的重新啓動常式。

執行產品更新，並在下次系統重新開機後需要重新啓動電腦：在使用者啓動電腦及登入之後，執行更新和重新啓動。建議對這個選項使用自動重新啓動常式。

重新啓動設定

在以下秒數後重新啓動電腦

此選項一經啓用，執行產品更新之後，就會在指定間隔**自動**執行必要的重新啓動。這時會出現倒數計時訊息，其中沒有取消電腦重新啓動的選項。

每 **n** 秒顯示一次重新啓動提醒訊息

此選項一經啓用，執行產品更新之後，**不會**自動執行必要的重新啓動。在指定間隔，您會收到沒有取消選項的重新啓動通知。這些通知可讓您確認電腦重新啓動或選取 "**[再次提醒我]**"。

詢問是否要重新啓動電腦

此選項一經啓用，執行產品更新之後，**不會**自動執行必要的重新啓動。您將只會收到一則訊息，提供您選擇直接執行重新啓動或取消重新啓動常式。

不需詢問，直接重新啓動電腦

此選項一經啓用，執行產品更新之後，就會**自動**執行必要的重新啓動。您不會收到任何通知。

您可以經由網際網路上的網路伺服器，直接執行更新。

網路伺服器連線

<u>使用現有的連線 **(網路)**</u>

如果您是透過網路進行連線，會顯示此設定。

<u>使用下列連線</u>

如果您個別定義連線，會顯示此設定。

更新程式會自動偵測有哪些可用的連線選項。不可用的連線選項會反白顯示，而且無法啓用。例如，您可以透過 Windows 中的電話簿項目，手動建立撥號連線。

– **用戶**：輸入選取的帳戶使用者名稱。
– **密碼:**輸入此帳戶的密碼。爲了安全起見，您在此輸入的實際字元將以星號 (*) 取代。

注意
如果您忘記了現有的網際網路帳戶名稱或密碼，請連絡您的網際網路服務供應商。

注意
目前不提供透過所謂的撥接工具 (例如，SmartSurfer、Oleco 等等) 進行更新程式的自動撥接服務。

<u>終止爲更新設定的撥號連線</u>

此選項一經啓用，只要順利完成下載，就會立即再次自動中斷針對更新所進行的 RDT 連線。

注意
Vista 環境下無法使用此選項。在 Vista 環境下，爲更新作業開啓的撥接連線一律在順利完成下載之後立即終止。

13.9 一般

13.9.1 威脅類別

選取威脅類別

您的 AntiVir 可保護您免受電腦病毒的威脅。

此外，您可以依據下列延伸的威脅類別來進行掃描。

– 後門程式用戶端 (BDC)
– 撥號木馬程式 (DIALER)
– 遊戲 (GAMES)
– 惡作劇程式 (JOKES)
– 安全性隱私風險 (SPR)
– 廣告軟體/間諜軟體 (ADSPY)
– 少見的執行階段壓縮程式 (PCK)

– 雙重副檔名檔案 (HEUR-DBLEXT)
– 網路釣魚
– 應用程式 (APPL)

只要按一下相關方塊，就會啓用 (加上勾選標記) 或停用 (無勾選標記) 選取的類型。

<u>全部選取</u>

此選項一經啓用，就會啓用所有類型。

<u>預設值</u>

此按鈕會還原預先定義的預設值。

注意
如果停用某個類型，就不會再指出識別爲相關程式類型的檔案。報告檔案不會列出任何項目。

13.9.2 密碼

您可以使用密碼保障 AntiVir 程式在各方面的安全性。一旦密碼已經發行，每當您想要開啓保護的區域時，系統就會要求您輸入此密碼。

密碼

<u>輸入密碼</u>

在此輸入要求的密碼。爲了安全起見，您在此輸入的實際字元將以星號 (*) 取代。密碼長度上限爲 20 個字元。密碼一經發行，程式就會在輸入錯誤的密碼時拒絕存取。空白方塊代表「無密碼」。

<u>確認密碼</u>

在此再次輸入密碼，以確認以上輸入的密碼。爲了安全起見，您在此輸入的實際字元將以星號 (*) 取代。

注意
密碼區分大小寫！

受密碼保護的區域

您的 AntiVir 程式可以用密碼保護各方面的安全性。只要按一下相關方塊，就可以視需要針對個別區域停用或重新啓用密碼要求。

受密碼保護的區域	功能
控制中心	此選項一經啓用，便需要預先定義的密碼來啓動控制中心。
啓用/停用 Guard	此選項一經啓用，便需要使用預先定義的密碼來啓用或停用 AntiVir Guard。
啓用/停用 MailGuard	此選項一經啓用，便需要使用預先定義的密碼來啓用或停用 MailGuard。

啓用/停用 FireWall	此選項一經啓用，便需要使用預先定義的密碼來啓用或停用 FireWall。
啓用/停用 WebGuard	此選項一經啓用，便需要使用預先定義的密碼來啓用或停用 WebGuard。
啓用/停用家長監護功能	此選項一經啓用，便需要使用預先定義的密碼來啓用或停用家長監護。
隔離區	此選項一經啓用，便會啓用所有受到密碼保護的隔離區管理員區域。只要按一下相關方塊，就可以在要求下再次針對個別區域停用或重新啓用密碼查詢功能。
還原受影響的物件	此選項一經啓用，便需要預先定義密碼來還原物件。
重新掃描受影響的物件	此選項一經啓用，便需要預先定義密碼來重新掃描物件。
受影響物件的屬性	此選項一經啓用，便需要預先定義密碼來顯示物件屬性。
刪除受影響的物件	此選項一經啓用，便需要預先定義密碼來刪除物件。
傳送電子郵件至 Avira	此選項一經啓用，便需要預先定義密碼以將物件傳送至 Avira 惡意程式碼研究中心進行檢查。
複製受影響的物件	此選項一經啓用，便需要預先定義密碼來複製受影響的物件。
新增與修改工作	此選項一經啓用，便需要預先定義密碼來新增並修改在 [排程管理員] 中的物件。
開始更新產品	此選項一經啓用，便需要預先定義密碼來啓動 [更新] 功能表中的產品更新。
組態	此選項一經啓用，就需要先輸入預先定義的密碼才能進行程式組態。
啓用專家模式	此選項一經啓用，便需要使用預先定義的密碼來啓用或停用專家模式。
安裝/解除安裝	此選項一經啓用，就需要預先定義密碼以安裝或解除安裝程式。

13.9.3 安全性

更新

如果上次更新是在 n 天之前，則發出警示

在此方塊中，您可以輸入上次更新之後，允許經過的天數上限。經過此天數後，控制中心的 [狀態] 底下會顯示更新狀態的紅色圖示。

如果病毒定義檔已非最新狀態，顯示通知

此選項一經啓用，一旦病毒定義檔不是最新的，您就會收到警示。透過警示選項，您可以設定在上次更新超過 n 天後，要發出的警示時間間隔。

產品保護

注意
如果 Guard 尚未以使用者定義安裝選項完成安裝，您就無法使用產品保護選項。

保護處理序，避免意外終止

此選項一經啓用，會保護此程式的所有處理序免於遭到病毒與惡意程式碼的惡意終止，或是避免使用者透過 [工作管理員] 加以「強制」終止。此選項會啓用爲預設值。

進階處理序保護

此選項一經啓用，此程式的所有處理序都會受到進階選項保護，避免意外終止。進階程序保護比簡易密碼保護需要更多電腦資源。此選項會啓用爲預設值。若要停用此選項，您必須重新啓動電腦。

重要
密碼保護不適用於 Windows XP 64 位元！

警告
如果啓用處理序保護，則其他軟體產品可能會出現互動問題。請在這些情況下停用處理序保護。

保護檔案和登錄項目，避免操作

此選項一經啓用，會保護此程式的所有登錄項目與所有程式檔 (二進位與組態檔) 免於遭到操作。免於遭到操作代表預防使用者或外部程式寫入、刪除，以及在某些情況下，讀取登錄項目或是程式檔案。若要啓用此選項，您必須重新啓動電腦。

警告
請記住，一旦此選項停用，可能就無法修復遭受特定類型惡意軟體感染的電腦。

注意
此選項一經啓用，便只能透過使用者介面來進行對組態進行變更，包括對掃描或更新要求的變更。

重要
檔案和登錄項目保護不適用於 Windows XP 64 位元！

13.9.4 WMI

支援 Windows Management Instrumentation

Windows Management Instrumentation 是基本的 Windows 管理技巧，它運用指令碼與程式設計語言同時允許在本機與遠端讀取與寫入 Windows 系統上的設定。您的 AntiVir 程式支援 WMI 並透過介面提供相關資料 (狀態資訊、統計資料、報告、預計要求等等)、事件。WMI 可讓您選擇從

<u>啟用 **WMI** 支援</u>

此選項一經啟用，就可以透過 WMI 從程式下載作業資料。

13.9.5 Proxy

Proxy 伺服器

<u>不要使用 **Proxy** 伺服器</u>

此選項一經啟用，便無法透過 Proxy 伺服器建立對網路伺服器的連線。

<u>使用 **Windows** 系統設定</u>

此選項一經啟用，便會使用目前的 Windows 系統設定，經由 Proxy 伺服器連線至網路伺服器。設定 Windows 系統設定值，以便根據 **[控制台::網際網路選項::連線::LAN 設定]** 區段來使用 Proxy 伺服器。您也可以用 Internet Explorer，在 [其他功能] 功能表中存取 [網際網路] 選項。

警告
如果您要使用必須進行驗證的 Proxy 伺服器，則請在選項 *[使用此 Proxy 伺服器]* 下方輸入所有必要的資料。選項 *[使用 Windows 系統設定]* 只能用於不用驗證的 Proxy 伺服器。

<u>使用此 **Proxy** 伺服器</u>

如果您是經由 Proxy 伺服器設定網路伺服器連線，可在此輸入相關資訊。

<u>地址</u>

請輸入您在連線至網路伺服器時要使用的 Proxy 伺服器之電腦名稱或 IP 位址。

<u>連接埠</u>

請輸入您在連線至網路伺服器時要使用之 Proxy 伺服器的連接埠編號。

<u>登入名稱</u>

請輸入使用者名稱來登入 Proxy 伺服器。

<u>登入密碼</u>

在此輸入 Proxy 伺服器的相關登入密碼。為了安全起見，您在此輸入的實際字元將以星號 (*) 取代。

例如：

地址：	proxy.domain.com	連接埠：	8080
地址：	192.168.1.100	連接埠：	3128

13.9.6 目錄

暫存檔路徑

在此輸入方塊中，輸入程式將儲存其暫存檔的路徑。

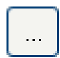
<u>使用預設系統設定</u>

此選項一經啓用，會使用系統設定來處理暫存檔案。

> **注意**
> 您可以查看系統儲存暫存檔案的位置爲何 – 例如，在 Windows XP 環境中，可以進入：[開始]/[設定]/[控制台]/[系統]/[進階]/[索引卡]/[進階]/[按鈕]/[環境變數]。""""此處會顯示目前登錄的使用者與系統變數 (TEMP、TMP) 的暫存檔變數 (TEMP、TMP)，與其相關數值。

<u>使用下列目錄</u>

此選項一經啓用，會使用輸入方塊中顯示的路徑。



此按鈕會開啓新的視窗，供您選取必要的暫存檔路徑。

<u>預設值</u>

此按鈕會還原預先定義的暫存檔路徑目錄。

13.9.7 活動

限制事件資料庫的大小

<u>限制事件數量上限爲 **n** 個項目</u>

此選項一經啓用，可將事件資料庫中所列的事件數量上限限定爲特定大小，可能的值爲：100 到 10000 個項目。如果輸入的數量超出此限，會從最舊的項目開始刪除。

<u>刪除超過以下天數的所有事件</u>

此選項一經啓用，經過特定期間之後會刪除事件資料庫中所列的事件，可能的值爲：1 至 90 天。系統預設會啓用此選項，並使用 30 天的預設值。

<u>無限制 **(手動刪除事件)**</u>

此選項一經啓用，便不會限制事件資料庫大小。不過，程式介面的 [事件] 底下最多顯示 20,000 個項目。

13.9.8 限制報告

限制報告份數

<u>限制數目上限爲</u>

此選項一經啓用，可將報告份數上限限定爲特定數量。允許介於 1 到 300 之間的值。如果超出此指定數量，會從最舊的報告開始刪除。

<u>刪除超過此天數的所有報告</u>

此選項一經啓用，會在經過特定天數後自動刪除報告。允許的值爲：1 至 90 天。系統預設會啓用此選項，並使用 30 天的預設值。

<u>無限制 **(手動刪除報告)**</u>

此選項一經啓用，便不會限制報告份數。

13.9.9 警示音

警示音

當掃描程式或 Guard 偵測到病毒或惡意程式碼，會以互動模式發出警示音。您現在可以選擇啓用或停用警示音，並選取其他 Wave 檔做爲警示音。

> **注意**
> 掃描程式的動作模式是在組態的掃描程式::掃描::偵測有所發現時採取的動作底下進行設定。Guard 的動作模式是在組態的 Guard::掃描::偵測有所發現時採取的動作底下進行設定。

<u>無警告</u>

此選項一經啓用，當掃描程式或 Guard 偵測到病毒時，不會發出任何警示音。

<u>使用 **PC** 喇叭 **(僅在互動式模式)**</u>

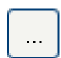
此選項一經啓用，當掃描程式或 Guard 偵測到病毒時，會發出預設的警示音訊號。警示音會從電腦'的內部喇叭發出。

<u>使用下列 **Wave** 檔 **(僅在互動式模式)**</u>

此選項一經啓用，當掃描程式或 Guard 偵測到病毒時，會發出選取的 Wave 檔警示音。選取的 Wave 檔會透過連接的外部喇叭播放。

<u>**Wave** 檔</u>

您可以在輸入方塊輸入自選的音訊檔名稱與關聯路徑。可輸入程式'預設警示訊號做爲標準設定。



此按鈕會開啓視窗，讓您透過檔案總管的協助選取所需的檔案。

<u>測試</u>

此按鈕可用來測試選取的 Wave 檔。

13.9.10 警告

您的 AntiVir 程式會針對特定事件產生所謂的上滑式訊息桌面通知，提供有關成功或失敗程式序列 (例如更新) 的資訊。您可以在 *[警告]* 中啓用或停用特定事件的通知。

利用桌面通知，您可以選擇直接在上滑式訊息停用通知。可以在 *[警告]* 中復原停用通知動作。

警告

<u>使用撥號連線時</u>

此選項一經啓用，一旦撥號木馬程式在您的電腦上透過電話或 ISDN 網路建立撥號連線時，您就會收到桌面通知警示。連線可能由不明且有害的撥號木馬程式所建立，而且可能是付費電話 (請參閱 病毒與其他資訊::威脅類別:撥號木馬程式)。

成功更新檔案時

此選項一經啓用，只要成功執行更新且更新檔案，您就會收到桌面通知。

更新失敗時

此選項一經啓用，只要更新失敗，您就會收到桌面通知：無法建立與下載伺服器的連線，或無法安裝更新檔案。

沒有必要更新

此選項一經啓用，每當啓動更新之後，卻因爲您的程式是最新版本而不需要安裝檔案時，您就會收到桌面通知。



live *free.*™